Discrete Mathematics

Mathematics

PDF generated using the open source mwlib toolkit. See http://code.pediapress.com/ for more information.
PDF generated at: Mon, 23 Apr 2012 14:07:22 UTC

Contents

Articles

Discrete Mathematics/Introduction 1
Discrete Mathematics/Set theory 1
Discrete Mathematics/Set theory/Page 2 12
Discrete Mathematics/Functions and relations 21
Discrete Mathematics/Number theory 31
Discrete Mathematics/Graph theory 45
Discrete Mathematics/Recursion 49
Discrete Mathematics/Axiomatic set theory 52
Discrete Mathematics/Zermelo-Frankel Axioms 52
Discrete Mathematics/Number representations 54
Discrete Mathematics/Modular arithmetic 59
Discrete Mathematics/Polynomials 64
Discrete Mathematics/Finite fields 68
Discrete Mathematics/Arithmetic Functions 70
Discrete Mathematics/Analytic Number Theory 71
Abstract Algebra/Group Theory 75
Abstract Algebra/Lattice theory 77
Abstract Algebra/Matroids 77
Abstract Algebra/Category theory 77
Abstract Algebra/Hypercomplex numbers 78
Abstract Algebra/Rings 79
Discrete Mathematics/Combinatory logic 82
Discrete Mathematics/Finite state automata 82
Discrete Mathematics/Selected problems 83
Discrete Mathematics/Axiom of choice 83
Discrete Mathematics/Naive set theory 84
Discrete Mathematics/Sieve of Eratosthenes 88
Discrete Mathematics 88

References

Article Sources and Contributors 91
Image Sources, Licenses and Contributors 92

Article Licenses

Discrete Mathematics/Introduction

Mathematics can help you solve many problems by training you to think well. This book will help you think well about **discrete** problems: problems like chess, in which the moves you make are exact, problems where tools like calculus fail because there's no continuity, problems that appear all the time in games, puzzles, and computer science.

We hope you'll enjoy discovering discrete mathematics here, and we hope you'll find this a good reference for quickly picking up the details you'll forget with time.

../Set theory/ >

Notice to contributors: If you wish to contribute images of any kind that contains labels, please use the Arial font, italic, at 16pts for consistency.

Discrete Mathematics/Set theory

Set Theory starts very simply: it examines whether an object *belongs*, or does *not belong*, to a *set* of objects which has been described in some non-ambiguous way. From this simple beginning, an increasingly complex (and useful!) series of ideas can be developed, which lead to notations and techniques with many varied applications.

Definition of a Set

The definition of a set sounds very vague at first. A ***set*** can be defined as a collection of ***things*** that are brought together because they obey a certain ***rule***.

These 'things' may be anything you like: numbers, people, shapes, cities, bits of text ..., literally anything.

The key fact about the 'rule' they all obey is that it must be *well-defined*. In other words, it enables us to say for sure whether or not a given 'thing' belongs to the collection. If the 'things' we're talking about are English words, for example, a well-defined rule might be:

> '... has 5 or more letters'

A rule which is not well-defined (and therefore couldn't be used to define a set) might be:

> '... is hard to spell'

Elements

A 'thing' that belongs to a given set is called an ***element*** of that set. For example:

> Henry VIII is an element of the set of Kings of England

Notation

Curly brackets $\{\ldots\}$ are used to stand for the phrase 'the set of ...'. These braces can be used in various ways. For example:

We may *list* the elements of a set:

$$\{-3,-2,-1,0,1,2,3\}$$

We may *describe* the elements of a set:

$$\{\text{ integers between } -3 \text{ and } 3 \text{ inclusive}\}$$

We may use an *identifier* (the letter x for example) to represent a *typical element*, a $|$ symbol to stand for the phrase 'such that', and then the rule or rules that the identifier must obey:

$$\{x|x \text{ is an integer and } |x| < 4\}$$

or

$$\{x|x \in \mathbb{Z}, |x| < 4\}$$

The last way of writing a set - called *set comprehension* notation - can be generalized as:

$x|P(x)$, where $P(x)$ is a statement (technically a *propositional function*) about x and the set is the collection of all elements x for which P is true.

The symbol $\in$ is used as follows:

$\in$ means 'is an element of ...'. For example: $\text{dog } \in \{\text{quadrupeds}\}$

$\notin$ means 'is not an element of ...'. For example: $\text{Washington DC} \notin \{\text{European capital cities}\}$

A set can be *finite*: $\{\text{British citizens}\}$

... or *infinite*: $\{7, 14, 21, 28, 35, \ldots\}$

(Note the use of the *ellipsis* $\cdots$ to indicate that the sequence of numbers continues indefinitely.)

Sets will usually be denoted using *upper case* letters: A , B , ...

Elements will usually be denoted using *lower case* letters: x , y , ...

Some Special Sets

Universal Set

The set of all the 'things' currently under discussion is called the ***universal set*** (or sometimes, simply the ***universe***). It is denoted by **U**.

The universal set doesn’t contain everything in the whole universe. On the contrary, it restricts us to just those things that are relevant at a particular time. For example, if in a given situation we’re talking about numeric values – quantities, sizes, times, weights, or whatever – the universal set will be a suitable set of numbers (see below). In another context, the universal set may be {alphabetic characters} or {all living people}, etc.

Empty set

The set containing no elements at all is called the ***null set***, or ***empty set***. It is denoted by a pair of empty braces: $\{\}$ or by the symbol $\varnothing$.

It may seem odd to define a set that contains no elements. Bear in mind, however, that one may be looking for solutions to a problem where it isn't clear at the outset whether or not such solutions even exist. If it turns out that there isn't a solution, then the set of solutions is empty.

For example:

If $U = \{\text{words in the English language}\}$ then $\{\text{words with more than 50 letters}\} = \varnothing$.

If $U = \{\text{whole numbers}\}$ then $\{x|x^2 = 10\} = \varnothing$.

Operations on the empty set

Operations performed on the empty set (as a set of things to be operated upon) can also be confusing. (Such operations are nullary operations.) For example, the sum of the elements of the empty set is zero, but the product of the elements of the empty set is one (see empty product). This may seem odd, since there are no elements of the empty set, so how could it matter whether they are added or multiplied (since “they” do not exist)? Ultimately, the results of these operations say more about the operation in question than about the empty set. For instance, notice that zero is the identity element for addition, and one is the identity element for multiplication.

Some special sets of numbers

Several sets are used so often, they are given special symbols.

The natural numbers

The 'counting' numbers (or whole numbers) starting at 1, are called the ***natural numbers***. This set is sometimes denoted by **N**. So **N** = {0, 1, 2, 3, ...}

Note that, when we write this set by hand, we can't write in **bold** type so we write an N in blackboard bold font: $\mathbb{N}$

Integers

All whole numbers, positive, negative and zero form the set of ***integers***. It is sometimes denoted by **Z**. So **Z** = {..., -3, -2, -1, 0, 1, 2, 3, ...}

In blackboard bold, it looks like this: $\mathbb{Z}$

Real numbers

If we expand the set of integers to include all decimal numbers, we form the set of ***real numbers***. The set of reals is sometimes denoted by **R**.

A real number may have a *finite* number of digits after the decimal point (e.g. 3.625), or an *infinite* number of decimal digits. In the case of an infinite number of digits, these digits may:

> recur; e.g. 8.127127127...
>
> ... or they may not recur; e.g. 3.141592653...

In blackboard bold: $\mathbb{R}$

Rational numbers

Those real numbers whose decimal digits are finite in number, or which recur, are called ***rational numbers***. The set of rationals is sometimes denoted by the letter **Q**.

A rational number can always be written as exact fraction *p*/*q*; where *p* and *q* are integers. If *q* equals 1, the fraction is just the integer *p*. Note that *q* may NOT equal zero as the value is then undefined.

> For example: 0.5, -17, 2/17, 82.01, 3.282828... are all rational numbers.

In blackboard bold: $\mathbb{Q}$

Irrational numbers

If a number *can't* be represented exactly by a fraction *p*/*q*, it is said to be ***irrational***.

> Examples include: √2, √3, π.

Set Theory Exercise 1

Click the link for Set Theory Excercise 1

Relationships between Sets

We’ll now look at various ways in which sets may be related to one another.

Equality

Two sets *A* and *B* are said to be ***equal*** if and only if they have exactly the same elements. In this case, we simply write:

$A = B$

Note two further facts about equal sets:

The *order* in which elements are listed does not matter.

If an element is listed *more than once*, any repeat occurrences are ignored.

So, for example, the following sets are all equal:

$\{1, 2, 3\} = \{3, 2, 1\} = \{1, 1, 2, 3, 2, 2\}$

(You may wonder why one would ever come to write a set like $\{1, 1, 2, 3, 2, 2\}$. You may recall that when we defined the *empty set* we noted that there may be no solutions to a particular problem - hence the need for an empty set. Well, here we may be trying several different approaches to solving a problem, some of which in fact lead us to the same solution. When we come to consider the *distinct* solutions, however, any such repetitions would be ignored.)

Subsets

If all the elements of a set A are also elements of a set B, then we say that A is a ***subset*** of B, and we write:

$A \subseteq B$

For example:

If $T = \{2, 4, 6, 8, 10\}$ and $E = \{$even integers$\}$, then $T \subseteq E$

If $A = \{$alphanumeric characters$\}$ and $P = \{$printable characters$\}$, then $A \subseteq P$

If $Q = \{$quadrilaterals$\}$ and $F = \{$plane figures bounded by four straight lines$\}$, then $Q \subseteq F$

Notice that $A \subseteq B$ does not imply that B must necessarily contain extra elements that are not in A; the two sets could be equal – as indeed Q and F are above. However, if, in addition, B does contain at least one element that isn’t in A, then we say that A is a ***proper subset*** of B. In such a case we would write:

$A \subset B$

In the examples above:

E contains 12, 14, ... , so $T \subset E$

P contains \$, ;, &, ..., so $A \subset P$

But Q and F are just different ways of saying the same thing, so $Q = F$

The use of $\subset$ and $\subseteq$ is clearly analogous to the use of $<$ and $\leq$ when comparing two numbers.

Notice also that *every* set is a subset of the *universal set*, and the *empty set* is a subset of *every* set.

(You might be curious about this last statement: how can the empty set be a subset of *anything*, when it doesn’t contain any elements? The point here is that for every set A, the empty set **doesn’t** contain any elements that **aren't** in A. So $\emptyset \subseteq A$ for all sets A.)

Finally, note that if $A \subseteq B$ and $B \subseteq A$ then A and B must contain exactly the same elements, and are therefore equal. In other words:

If $A \subseteq B$ and $B \subseteq A$ then $A = B$

Disjoint

Two sets are said to be ***disjoint*** if they have no elements in common. For example:

> If A = {even numbers} and B = {1, 3, 5, 11, 19}, then A and B are disjoint.

Venn Diagrams

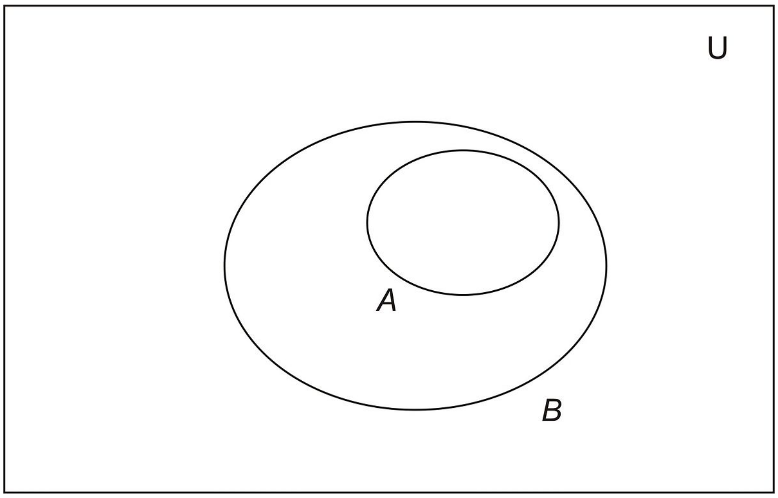
A *Venn diagram* can be a useful way of illustrating relationships between sets.

In a Venn diagram:

> The *universal set* is represented by a *rectangle*. Points inside the rectangle represent elements that are in the universal set; points outside represent things not in the universal set. You can think of this rectangle, then, as a 'fence' keeping unwanted things out - and concentrating our attention on the things we're talking about.
>
> Other sets are represented by *loops*, usually oval or circular in shape, drawn inside the rectangle. Again, points inside a given loop represent elements in the set it represents; points outside represent things *not* in the set.

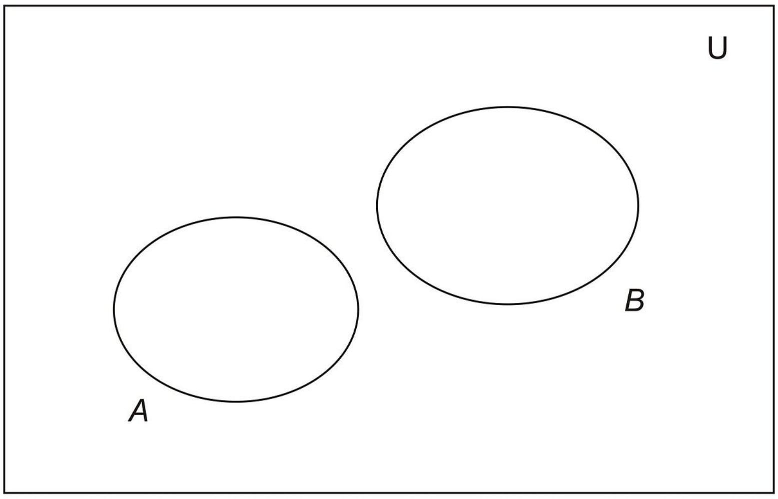
On the left, the sets A and B are disjoint, because the loops don't overlap.

On the right A is a subset of B, because the loop representing set A is entirely enclosed by loop B.



$A \subset B$

Venn diagrams: Fig. 2

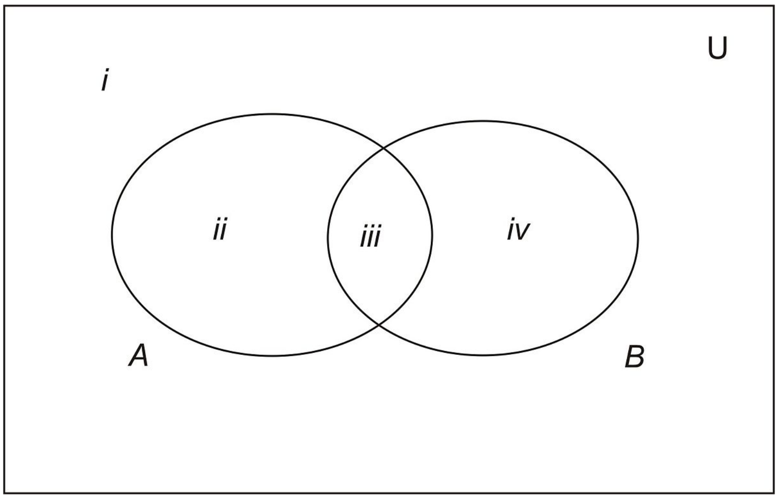


A and *B* are *disjoint*

Venn diagrams: Fig. 1

Venn diagrams: Worked Examples

Example 1



Venn diagrams: Fig. 3

Fig. 3 represents a Venn diagram showing two sets *A* and *B*, in the general case where nothing is known about any relationships between the sets.

Note that the rectangle representing the universal set is divided into four regions, labelled *i*, *ii*, *iii* and *iv*.

What can be said about the sets *A* and *B* if it turns out that:

(a) region *ii* is empty?

(b) region *iii* is empty?

(a) If region *ii* is empty, then *A* contains no elements that are not in *B*. So *A* is a subset of *B*, and the diagram should be re-drawn like *Fig 2* above.

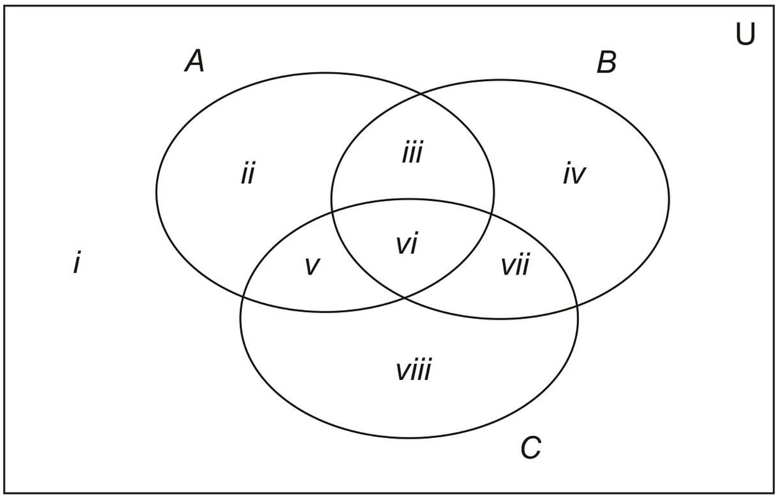
(b) If region *iii* is empty, then *A* and *B* have no elements in common and are therefore disjoint. The diagram should then be re-drawn like *Fig 1* above.

Example 2

(a) Draw a Venn diagram to represent three sets *A*, *B* and *C*, in the general case where nothing is known about possible relationships between the sets.

(b) Into how many regions is the rectangle representing **U** divided now?

(c) Discuss the relationships between the sets *A*, *B* and *C*, when various combinations of these regions are empty.



Venn diagrams: Fig. 4

(a) The diagram in *Fig. 4* shows the general case of three sets where nothing is known about any possible relationships between them.

(b) The rectangle representing **U** is now divided into 8 regions, indicated by the Roman numerals *i* to *viii*.

(c) Various combinations of empty regions are possible. In each case, the Venn diagram can be re-drawn so that empty regions are no longer included. For example:

If region *ii* is empty, the loop representing *A* should be made smaller, and moved inside *B* and *C* to eliminate region *ii*.

If regions *ii*, *iii* and *iv* are empty, make *A* and *B* smaller, and move them so that they are both inside *C* (thus eliminating all three of these regions), but do so in such a way that they still overlap each other (thus retaining region *vi*).

If regions *iii* and *vi* are empty, 'pull apart' loops *A* and *B* to eliminate these regions, but keep each loop overlapping loop *C*.

...and so on. Drawing Venn diagrams for each of the above examples is left as an exercise for the reader.

Example 3

The following sets are defined:

U = {1, 2, 3, …, 10}

A = {2, 3, 7, 8, 9}

B = {2, 8}

C = {4, 6, 7, 10}

Using the two-stage technique described below, draw a Venn diagram to represent these sets, marking all the elements in the appropriate regions.

The technique is as follows:

Draw a 'general' 3-set Venn diagram, like the one in *Example 2*.

Go through the elements of the universal set one at a time, once only, entering each one into the appropriate region of the diagram.

Re-draw the diagram, if necessary, moving loops inside one another or apart to eliminate any empty regions.

Don't begin by entering the elements of set *A*, then set *B*, then *C* – you'll risk missing elements out or including them twice!

Solution

After drawing the three empty loops in a diagram looking like *Fig. 4* (but without the Roman numerals!), go through each of the ten elements in **U** - the numbers 1 to 10 - asking each one three questions; like this:

First element: 1

Are you in *A*? No

Are you in *B*? No

Are you in *C*? No

A 'no' to all three questions means that the number 1 is outside all three loops. So write it in the appropriate region (region number *i* in *Fig. 4*).

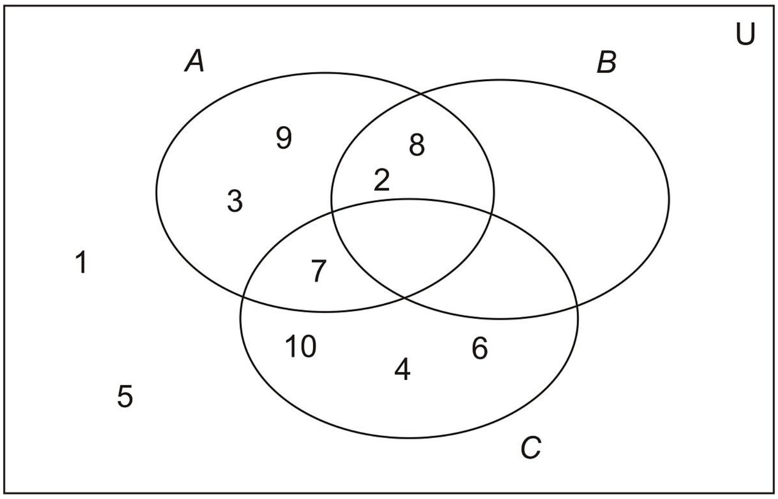
Second element: 2

Are you in *A*? Yes

Are you in *B*? Yes

Are you in *C*? No

Yes, yes, no: so the number 2 is inside *A* and *B* but outside *C*. Goes in region *iii* then.

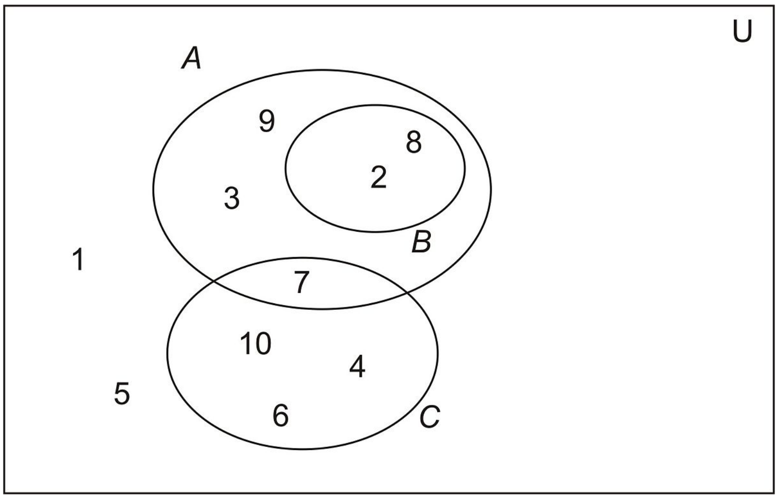


Venn diagrams: Fig. 5

...and so on, with elements 3 to 10.

The resulting diagram looks like *Fig. 5*.

The final stage is to examine the diagram for empty regions - in this case the regions we called *iv*, *vi* and *vii* in *Fig. 4* - and then re-draw the diagram to eliminate these regions. When we've done so, we shall clearly see the relationships between the three sets.



Venn diagrams: Fig. 6

So we need to:

> pull *B* and *C* apart, since they don't have any elements in common.
>
> push *B* inside *A* since it doesn't have any elements outside *A*.

The finished result is shown in *Fig. 6*.

The regions in a Venn Diagram and Truth Tables

Perhaps you've realized that adding an additional set to a Venn diagram *doubles* the number of regions into which the rectangle representing the universal set is divided. This gives us a very simple pattern, as follows:

> With one set loop, there will be just two regions: the inside of the loop and its outside.
>
> With two set loops, there'll be four regions.
>
> With three loops, there'll be eight regions.
>
> ...and so on.

It's not hard to see why this should be so. Each new loop we add to the diagram divides each existing region into two, thus doubling the number of regions altogether.

In *A*?	**In *B*?**	**In *C*?**
Y	Y	Y
Y	Y	N
Y	N	Y
Y	N	N
N	Y	Y
N	Y	N
N	N	Y
N	N	N

But there's another way of looking at this, and it's this. In the solution to *Example 3* above, we asked three questions of each element: *Are you in A? Are you in B?* and *Are you in C?* Now there are obviously two possible answers to each of these questions: *yes* and *no*. When we *combine* the answers to three questions like this, one after the other, there are then $2^3 = 8$ possible sets of answers altogether. Each of these eight possible combinations of answers corresponds to a different region on the Venn diagram.

The complete set of answers resembles very closely a *Truth Table* - an important concept in *Logic*, which deals with statements which may be *true* or *false*. The table on the right shows the eight possible combinations of answers for 3 sets *A*, *B* and *C*.

You'll find it helpful to study the patterns of Y's and N's in each column.

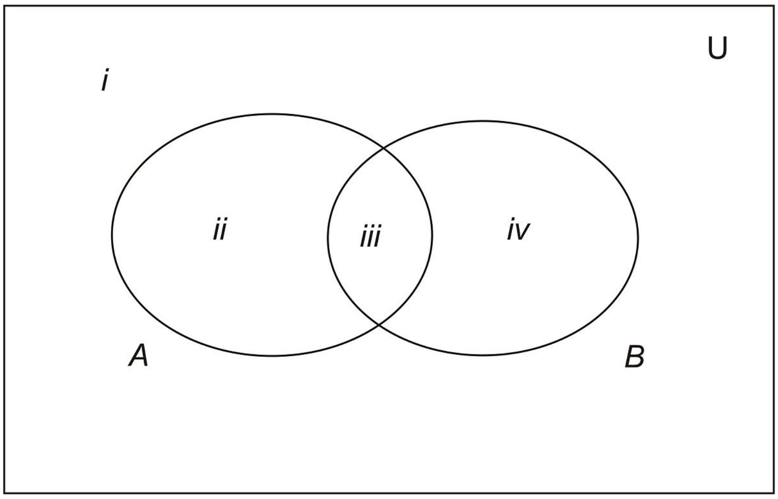
> As you read down column *C*, the letter changes on every row: Y, N, Y, N, Y, N, Y, N
>
> Reading down column *B*, the letters change on every other row: Y, Y, N, N, Y, Y, N, N
>
> Reading down column *A*, the letters change every four rows: Y, Y, Y, Y, N, N, N, N

Set Theory Exercise 2

Click link for Set Theory Exercise 2.

Operations on Sets

Just as we can combine two numbers to form a third number, with operations like 'add', 'subtract', 'multiply' and 'divide', so we can combine two sets to form a third set in various ways. We'll begin by looking again at the Venn diagram which shows two sets *A* and *B* in a general position, where we don't have any information about how they may be related.



Venn diagrams: Fig. 7

In *A*?	In *B*?	Region
Y	Y	*iii*
Y	N	*ii*
N	Y	*iv*
N	N	*i*

The first two columns in the table on the right show the four sets of possible answers to the questions *Are you in A?* and *Are you in B?* for two sets *A* and *B*; the Roman numerals in the third column show the corresponding region in the Venn diagram in *Fig. 7*.

Intersection

Region *iii*, where the two loops overlap (the region corresponding to 'Y' followed by 'Y'), is called the *intersection* of the sets A and B. It is denoted by $A \cap B$. So we can define intersection as follows:

> The ***intersection*** of two sets A and B, written $A \cap B$, is the set of elements that are in A **and** in B.

(Note that in symbolic logic, a similar symbol, $\wedge$, is used to connect two logical propositions with the **AND** operator.)

For example, if $A = \{1, 2, 3, 4\}$ and $B = \{2, 4, 6, 8\}$, then $A \cap B = \{2, 4\}$.

We can say, then, that we have combined two sets to form a third set using the *operation of intersection*.

Union

In a similar way we can define the *union* of two sets as follows:

> The ***union*** of two sets A and B, written $A \cup B$, is the set of elements that are in A **or** in B (or both).

The union, then, is represented by regions *ii*, *iii* and *iv* in *Fig. 7*.

(Again, in logic a similar symbol, $\vee$, is used to connect two propositions with the **OR** operator.)

> So, for example, $\{1, 2, 3, 4\} \cup \{2, 4, 6, 8\} = \{1, 2, 3, 4, 6, 8\}$.

You'll see, then, that in order to get into the intersection, an element must answer 'Yes' to *both* questions, whereas to get into the union, *either* answer may be 'Yes'.

The $\cup$ symbol looks like the first letter of 'Union' and like a cup that will hold a lot of items. The $\cap$ symbol looks like a spilled cup that won't hold a lot of items, or possibly the letter 'n', for i'n'tersection. Take care not to confuse the two.

Difference

> The ***difference*** of two sets A and B (also known as the ***set-theoretic difference*** of A and B, or the ***relative complement*** of B in A) is the set of elements that are **in** A **but not in** B.

This is written A - B, or sometimes $A \setminus$ B.

The elements in the difference, then, are the ones that answer 'Yes' to the first question *Are you in A?*, but 'No' to the second *Are you in B?*. This combination of answers is on row 2 of the above table, and corresponds to region *ii* in *Fig.7*.

> For example, if $A = \{1, 2, 3, 4\}$ and $B = \{2, 4, 6, 8\}$, then $A - B = \{1, 3\}$.

Complement

So far, we have considered operations in which *two* sets combine to form a third: *binary* operations. Now we look at a *unary* operation - one that involves just *one* set.

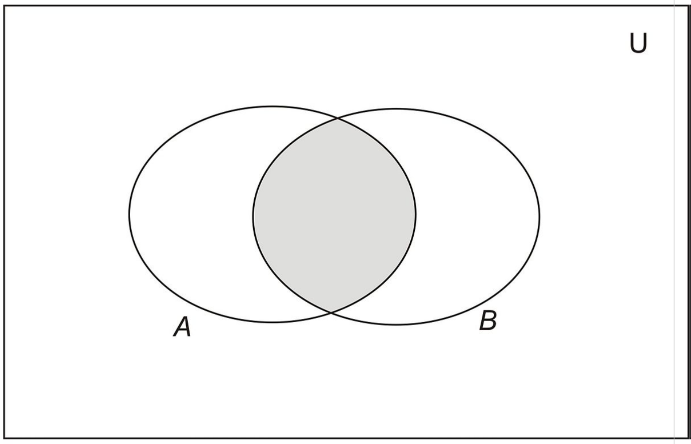
> The set of elements that are **not** in a set A is called the ***complement*** of A. It is written A' (or sometimes A^{C}, or $\bar{A}$).

Clearly, this is the set of elements that answer 'No' to the question *Are you in A?*.

> For example, if $\mathbf{U} = \mathbf{N}$ and A = {odd numbers}, then A' = {even numbers}.

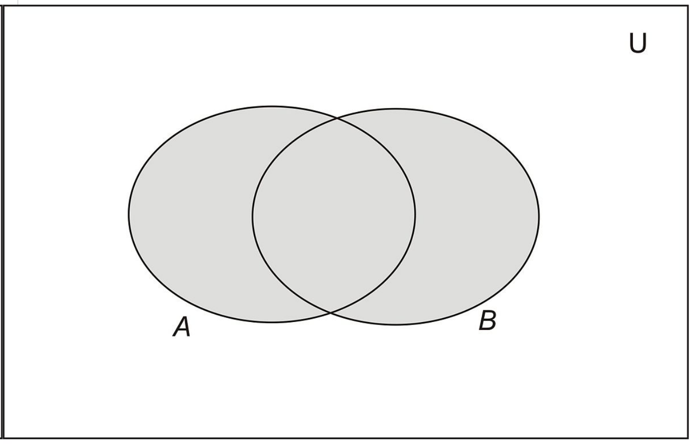
Notice the spelling of the word *complement*: its literal meaning is 'a complementary item or items'; in other words, 'that which completes'. So if we already have the elements of A, the complement of A is the set that *completes* the universal set.

Summary



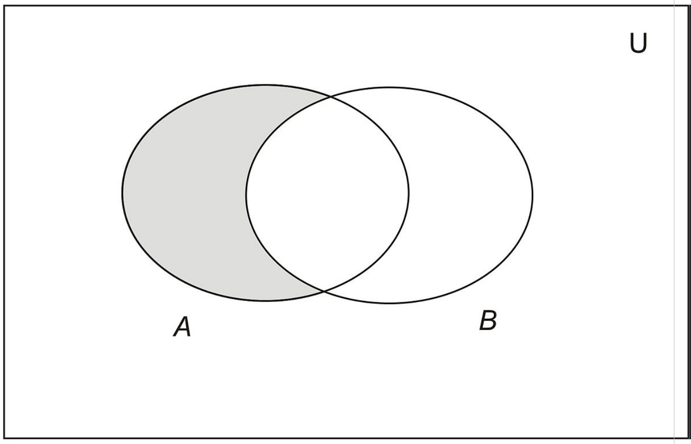
$A \cap B$

Intersection: things that are in *A* **and** in *B*



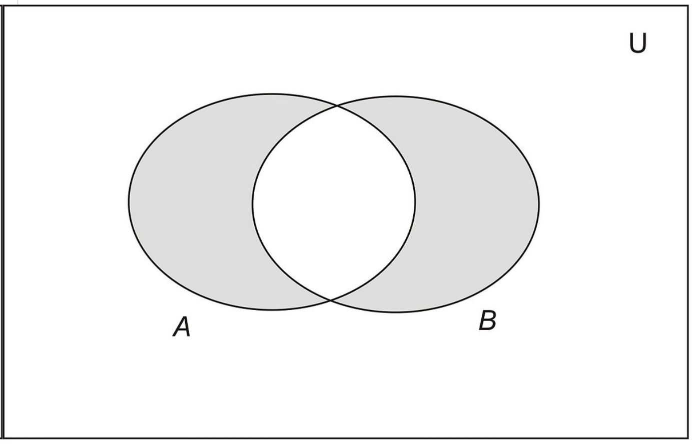
$A \cup B$

Union: things that are in *A* **or** in *B* (or both)



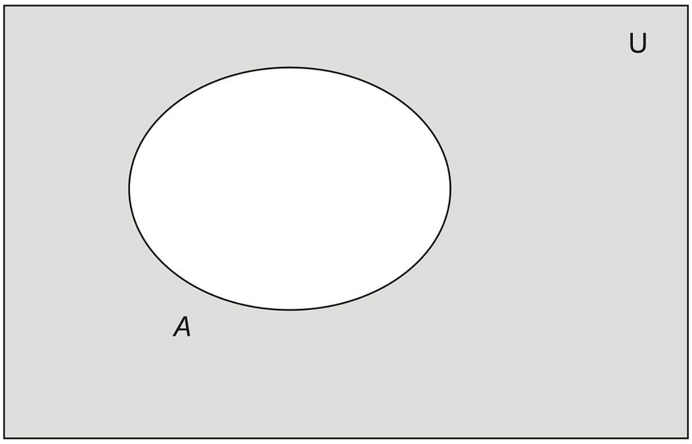
$A - B$

Difference: things that are in *A* **and not** in *B*



$A \Delta B$

Symmetric Difference: things that are in *A* **or** in *B* **but not** both



A'

Complement: things that are **not** in *A*

Cardinality

Finally, in this section on *Set Operations* we look at an operation on a set that yields not another set, but an integer.

> The ***cardinality*** of a finite set A, written | A | (sometimes #(A) or n(A)), is the number of (distinct) elements in A. So, for example:
>
> If A = {lower case letters of the alphabet}, | A | = 26.

Generalized set operations

If we want to denote the intersection or union of n sets, A_1, A_2, ..., A_n (where we may not know the value of n) then the following *generalized set notation* may be useful:

$$A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i$$

$$A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{i=1}^{n} A_i$$

In the symbol $\bigcap_{i=1}^{n} A_i$, then, i is a variable that takes values from 1 to n, to indicate the repeated intersection of all the sets A_1 to A_n.

Set Theory Exercise 3

Click link for Set Theory Exercise 3

Set Theory Page 2

Set Theory continues on Page 2.

Previous topic: ../Introduction/ | Contents:Discrete Mathematics | Next topic: ../Functions and relations/

Discrete Mathematics/Set theory/Page 2

This page is a continuation of Discrete_Mathematics/Set_theory. It may be omitted at a first reading.

Power Sets

The ***power set*** of a set A is the set of all its subsets (including, of course, itself and the empty set). It is denoted by **P**(A).

Using set comprehension notation, **P**(A) can be defined as

> $\mathbf{P}(A) = \{ Q \mid Q \subseteq A \}$

Example 4

> Write down the power sets of A if:

(a) $A = \{1, 2, 3\}$

(b) $A = \{1, 2\}$

(c) $A = \{1\}$

(d) $A = \emptyset$

Solution

(a) $\mathbf{P}(A) = \{ \{1, 2, 3\}, \{2, 3\}, \{1, 3\}, \{1, 2\}, \{1\}, \{2\}, \{3\}, \emptyset \}$

(b) $\mathbf{P}(A) = \{ \{1, 2\}, \{1\}, \{2\}, \emptyset \}$

(c) $\mathbf{P}(A) = \{ \{1\}, \emptyset \}$

(d) **P**(*A*) = { ø }

Cardinality of a Power Set

Look at the cardinality of the four sets in *Example 4*, and the cardinality of their corresponding power sets. They are:

	| *A* |	| **P**(*A*) |
(a)	3	8
(b)	2	4
(c)	1	2
(d)	0	1

Clearly, there's a simple rule at work here: expressed as powers of 2, the cardinalities of the power sets are 2^3, 2^2, 2^1 and 2^0.

It looks as though we have found a rule that if | *A* | = *k*, then | **P**(*A*) | = 2^k. But can we see why?

Well, the elements of the power set of *A* are all the possible subsets of *A*. Any one of these subsets can be formed in the following way:

> Choose any element of *A*. We may decide to *include* this in our subset, or we may *omit* it. There are therefore 2 ways of dealing with this first element of *A*.
>
> Now choose a second element of *A*. As before, we may include it, or omit it from our subset: again a choice of 2 ways of dealing with this element.
>
> ...and so on through all *k* elements of *A*.

Now the fundamental principle of combinatorics tells us that if we can do each of *k* things in 2 ways, then the total number of ways of doing them all, one after the other, is 2^k.

Each one of these 2^k combinations of decisions - including elements or omitting them - gives us a different subset of *A*. There are therefore 2^k different subsets altogether.

So if | *A* | = *k*, then | **P**(*A*) | = 2^k.

The Foundational Rules of Set Theory

The laws listed below can be described as the Foundational Rules of Set Theory. We derive them by going back to the definitions of intersection, union, universal set and empty set, and by considering whether a given element is in, or not in, one or more sets.

The Idempotent Laws

As an example, we'll consider the *'I heard you the first time' Laws* – more correctly called the *Idempotent Laws* - which say that:

> $A \cap A = A$ and $A \cup A = A$

This law might be familiar to you if you've studied logic. The above relationship is comparable to the tautology.

These look pretty obvious, don't they? A simple explanation for the intersection part of these laws goes something like this:

The intersection of two sets *A* and *B* is defined as just those elements that are in *A* and in *B*. If we replace *B* by *A* in this definition we get that the intersection of *A* and *A* is the set comprising just those elements that are in *A* and in *A*. Obviously, we don't need to say this twice (*I heard you the first time*), so we can simply say that the intersection of *A* and *A* is the set of elements in *A*. In other words:

> $A \cap A = A$

We can derive the explanation for $A \cup A = A$ in a similar way.

De Morgan's Laws

There are two laws, called *De Morgan's Laws*, which tell us how to remove brackets, when there's a *complement* symbol - ′ - outside. One of these laws looks like this:

$(A \cup B)' = A' \cap B'$

(If you've done Exercise 3, question 4, you may have spotted this law already from the Venn Diagrams.)

Look closely at how this Law works. The complement symbol after the bracket affects *all three* symbols inside the bracket when the brackets are removed:

A becomes A'

B becomes B'

and $\cup$ becomes $\cap$.

To prove this law, note first of all that when we defined a subset we said that if

$A \subseteq B$ and $B \subseteq A$, then $A = B$

So we prove:

(i) $(A \cup B)' \subseteq A' \cap B'$

and then the other way round:

(ii) $A' \cap B' \subseteq (A \cup B)'$

The proof of (i) goes like this:

Let's pick an element at random $x \in (A \cup B)'$. We don't know anything about x; it could be a number, a function, or indeed an elephant. All we do know about x, is that

$x \in (A \cup B)'$

So

$x \notin (A \cup B)$

because that's what complement means.

This means that x answers *No* to both questions *Are you in A?* and *Are you in B?* (otherwise it *would* be in the union of A and B). Therefore

$x \notin A$ and $x \notin B$

Applying complements again we get

$x \in A'$ and $x \in B'$

Finally, if something is in two sets, it must be in their intersection, so

$x \in A' \cap B'$

So, any element we pick at random from $(A \cup B)'$ is definitely in $A' \cap B'$. So by definition

$(A \cup B)' \subseteq A' \cap B'$

The proof of (ii) is similar:

First, we pick an element at random from the first set, $x \in A' \cap B'$

Using what we know about intersections, that means

$x \in A'$ and $x \in B'$

So, using what we know about complements,

$x \notin A$ and $x \notin B$

And if something is in neither A nor B, it can't be in their union, so

$$x \notin A \cup B$$

So, finally:

$$x \in (A \cup B)'$$

So:

$$A' \cap B' \subseteq (A \cup B)'$$

We've now proved (i) and (ii), and therefore:

$$(A \cup B)' = A' \cap B'$$

This gives you a taste for what's behind these laws. So here they all are.

The Laws of Sets

Commutative Laws

$$A \cap B = B \cap A$$

$$A \cup B = B \cup A$$

Associative Laws

$$(A \cap \mathrm{B}) \cap \mathrm{C} = A \cap (B \cap \mathrm{C})$$

$$(A \cup \mathrm{B}) \cup \mathrm{C} = A \cup (B \cup \mathrm{C})$$

Distributive Laws

$$A \cap (B \cup \mathrm{C}) = (A \cap \mathrm{B}) \cup (A \cap \mathrm{C})$$

$$A \cup (B \cap \mathrm{C}) = (A \cup \mathrm{B}) \cap (A \cup \mathrm{C})$$

Idempotent Laws

$$A \cap A = A$$

$$A \cup A = A$$

Identity Laws

$$A \cup \varnothing = A$$

$$A \cap \mathbf{U} = A$$

$$A \cup \mathbf{U} = \mathbf{U}$$

$$A \cap \varnothing = \varnothing$$

Involution Law

$$(A')' = A$$

Complement Laws

$$A \cup A \mathbf{= 'U}$$

$$A \cap A' = \varnothing$$

$$\mathbf{U}' = \varnothing$$

$$\varnothing' = \mathbf{U}$$

De Morgan's Laws

$$(A \cap B)' = A' \cup B'$$

$$(A \cup B)' = A' \cap B'$$

Duality and Boolean Algebra

You may notice that the above *Laws of Sets* occur in pairs: if in any given law, you exchange ∪ for ∩ and vice versa (and, if necessary, swap **U** and Ø) you get another of the laws. The 'partner laws' in each pair are called *duals*, each law being the dual of the other.

For example, each of De Morgan's Laws is the dual of the other.

The first complement law, $A \cup A' = \mathbf{U}$, is the dual of the second: $A \cap A' = \emptyset$.

... and so on.

This is called the ***Principle of Duality***. In practical terms, it means that you only need to remember *half* of this table!

This set of laws constitutes the axioms of a ***Boolean Algebra***. See Boolean Algebra [1] for more.

Proofs using the Laws of Sets

We may use these laws - and only these laws - to determine whether other statements about the relationships between sets are true or false. Venn diagrams may be helpful in suggesting such relationships, but only a proof based on these laws will be accepted by mathematicians as rigorous.

Example 5

Using the Laws of Sets, prove that the set $(A \cup B) \cap (A' \cap B)'$ is simply the same as the set A itself. State carefully which Law you are using at each stage.

Before we begin the proof, a few do's and don't's:

Do start with the single expression $(A \cup B) \cap (A' \cap B)'$, and aim to change it into simply A.	**Don't** begin by writing down the whole equation $(A \cup B) \cap (A' \cap B)' = A$ – that's what we must end up with.
Do change just one part of the expression at a time, using just one of the set laws at a time.	**Don't** miss steps out, and change two things at once.
Do keep the equals signs underneath one another.	**Don't** allow your work to become untidy and poorly laid out.
Do state which law you have used at each stage.	**Don't** take even the simplest step for granted.

Solution

		Law Used
$(A \cup B) \cap (A' \cap B)'$	$= (A \cup B) \cap ((A')' \cup B')$	De Morgan's
	$= (A \cup B) \cap (A \cup B')$	Involution
	$= A \cup (B \cap B')$	Distributive
	$= A \cup \emptyset$	Complement
	$= A$	Identity

We have now proved that $(A \cup B) \cap (A' \cap B)' = A$ whatever the sets A and B contain. A statement like this – one that is true for all values of A and B – is sometimes called an ***identity***.

Hints on Proofs

There are no foolproof methods with these proofs – practice is the best guide. But here are a few general hints.

Start with the more complicated side of the equation, aiming to simplify it into the other side.

Look for places where the Distributive Law will result in a simplification (like factorising in 'ordinary' algebra - see the third line in *Example 5* above).

You'll probably use De Morgan's Law to get rid of a ' symbol from outside a bracket.

Sometimes you may need to 'complicate' an expression before you can simplify it, as the next example shows.

Example 6

Use the Laws of Sets to prove that $A \cup (A \cap B) = A$.

Looks easy, doesn’t it? But you can go round in circles with this one. (Try it first before reading the solution below, if you like.) The key is to 'complicate' it a bit first, by writing the first A as $A \cap \mathbf{U}$ (using one of the Identity Laws).

Solution

		Law Used
$A \cup (A \cap B)$	$= (A \cap \mathbf{U}) \cup (A \cap B)$	Identity
	$= A \cap (\mathbf{U} \cup B)$	Distributive
	$= A \cap (B \cup \mathbf{U})$	Commutative
	$= A \cap \mathbf{U}$	Identity
	$= A$	Identity

Set Theory Exercise 4

Click link for Set Theory Exercise 4.

Cartesian Products

Ordered pairs

To introduce this topic, we look first at a couple of examples that use the principle of combinatorics that we noted earlier (see Cardinality); namely, that if an event R can occur in r ways and a second event S can then occur in s ways, then the total number of ways that the two events, R followed by S, can occur is $r \times s$. This is sometimes called the *r-s Principle*.

Example 7

MENU

Main Course

Poached Halibut

Roast Lamb

Vegetable Curry

Lasagne

Dessert

Fresh Fruit Salad

Apple Pie

Gateau

How many different meals – Main Course followed by Dessert - can be chosen from the above menu?

Solution

Since we may choose the main course in four ways, and then the dessert in three ways to form a different combination each time, the answer, using the *r-s Principle*, is that there are $4 \times 3 = 12$ different meals.

Example 8

You're getting ready to go out. You have 5 different (clean!) pairs of underpants and two pairs of jeans to choose from. In how many ways can you choose to put on a pair of pants and some jeans?

Solution

Using the *r-s Principle*, there are $5 \times 2 = 10$ ways in which the two can be chosen, one after the other.

In each of the two situations above, we have examples of ***ordered pairs***. As the name says, an ordered pair is simply a pair of 'things' arranged in a certain order. Often the order in which the things are chosen is arbitrary ‒ we simply have to decide on a convention, and then stick to it; sometimes the order really only works one way round.

In the case of the meals, most people choose to eat their main course first, and then dessert. In the clothes we wear, we put on our underpants before our jeans. You are perfectly free to fly in the face of convention and have your dessert before the main course - or to wear your underwear on top of your trousers - but you'll end up with different sets of ordered pairs if you do. And, of course, you'll usually have a lot of explaining to do!

The two 'things' that make up an ordered pair are written in round brackets, and separated by a comma; like this:

(Lasagne, Gateau)

You will have met ordered pairs before if you've done coordinate geometry. For example, (2, 3) represents the point 2 units along the *x*-axis and 3 units up the *y*-axis. Here again, there's a convention at work in the order of the numbers: we use alphabetical order and put the *x*-coordinate before the *y*-coordinate. (Again, you could choose to do your coordinate geometry the other way round, and put *y* before *x*, but once again, you'd have a lot of explaining to do!)

Using set notation, then, we could describe the situation in *Example 7* like this:

$M = \{\text{main courses}\}$, $D = \{\text{desserts}\}$, $C = \{\text{complete meals}\}$.

Then C could be written as:

$C = \{ (m, d) \mid m \in M \text{ and } d \in D \}$.

C is called the ***set product*** or ***Cartesian product*** of M and D, and we write:

$C = M \times D$

(read 'C equals M cross D')

Suppose that the menu in *Example 7* is expanded to include a starter, which is either soup or fruit juice. How many complete meals can be chosen now?

Well, we can extend the *r-s Principle* to include this third choice, and get $2 \times 4 \times 3 = 24$ possible meals.

If $S = \{\text{soup, fruit juice}\}$, then we can write:

$C = S \times M \times D$

An element of this set is an *ordered triple*: (starter, main course, dessert). Notice, then, that the order in which the individual items occur in the triple is the same as the order of the sets from which they are chosen: $S \times M \times D$ does not give us the same set of ordered triples as $M \times D \times S$.

Ordered *n*-tuples

In general, if we have *n* sets: $A_1, A_2, ..., A_n$, then their Cartesian product is defined by:

$$A_1 \times A_2 \times ... \times A_n = \{ (a_1, a_2, ..., a_n) \mid a_1 \in A_1, a_2 \in A_2, ..., a_n \in A_n) \}$$

and $(a_1, a_2, ..., a_n)$ is called an ***ordered n-tuple***.

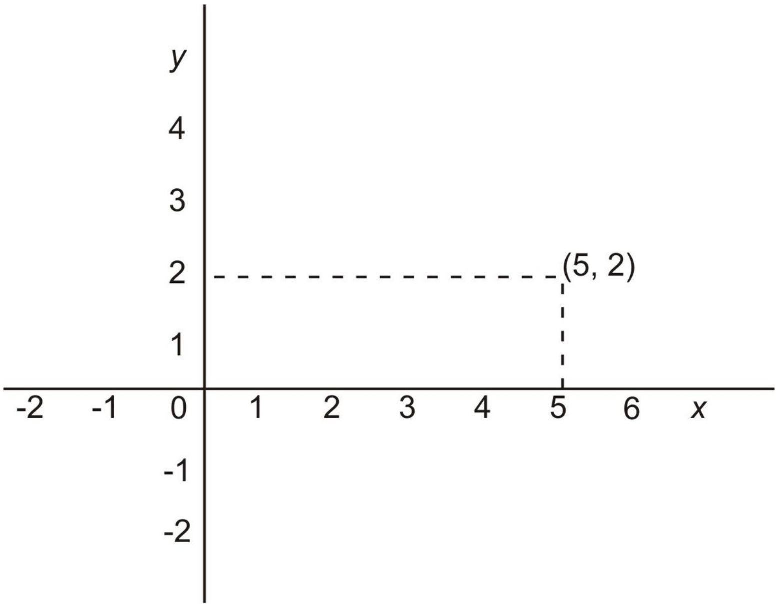
Notation

$A_1 \times A_2 \times ... \times A_n$ is sometimes written:

$$\times_{i=1}^{n} A_i$$

The Cartesian Plane

You probably know already the way in which a point in a plane may be represented by an ordered pair. The diagram in *Fig. 8* illustrates a *Cartesian Plane*, showing the point represented by the ordered pair (5, 2).



The Cartesian Plane: Fig. 8

The lines are called *axes*: the *x*-axis and the *y*-axis. The point where they meet is called the *origin*. The point (5, 2) is then located as follows: start at the origin; move 5 units in the direction of the *x*-axis, and then 2 units in the direction of the *y*-axis.

Using set notation:

If X = {numbers on the *x*-axis} and Y = {numbers on the *y*-axis}, then:

$$(5, 2) \in X \times Y$$

and, indeed, if X = {all real numbers}, and Y = {all real numbers} then $X \times Y$ as a whole represents *all* the points in the *x*-*y* plane.

(This is why you will sometimes see the *x*-*y* plane referred to as $\mathbf{R}^2$, where $\mathbf{R}$ = {real numbers}.)

Example 9

It is believed that, if A, B, P and Q are sets where $B \subset A$ and $Q \subset P$, then:

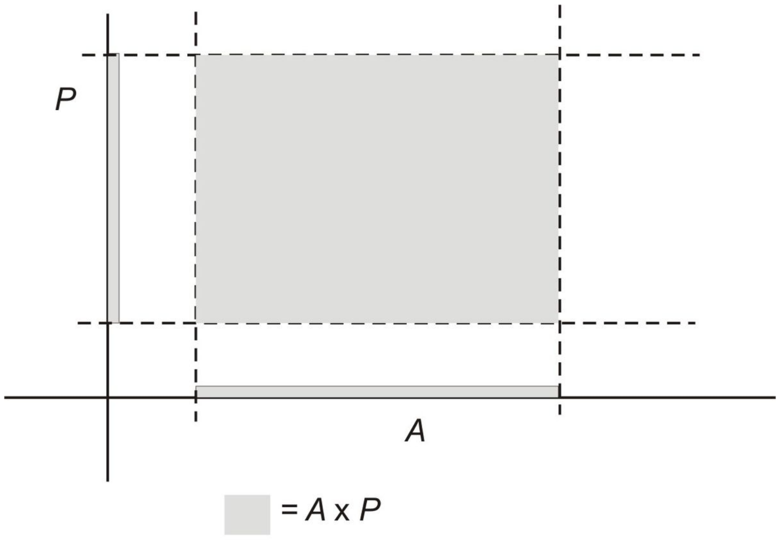
$$B \times Q \subset A \times P$$

Use a carefully shaded and labelled Cartesian diagram to investigate this proposition.

Solution

Bearing in mind what we said above about the ordered pairs in $X \times Y$ corresponding to points in the *x*-*y* plane, if we want to represent a Cartesian product like $A \times P$ on a diagram, we shall need to represent the individual sets A and P as sets of points on the *x*- and *y*- axes respectively.

The region representing the Cartesian product $A \times P$ is then represented by the points whose *x*- and *y*-coordinates lie within these sets A and P. Like this:

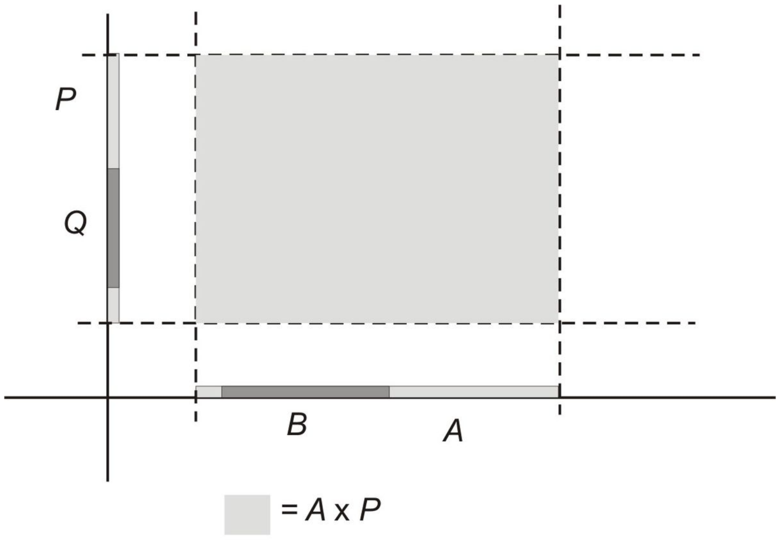


The Cartesian Plane: Fig. 9a

The same can also be said about *B* and *Q*: *B* must lie on the *x*-axis, and *Q* on the *y*-axis.

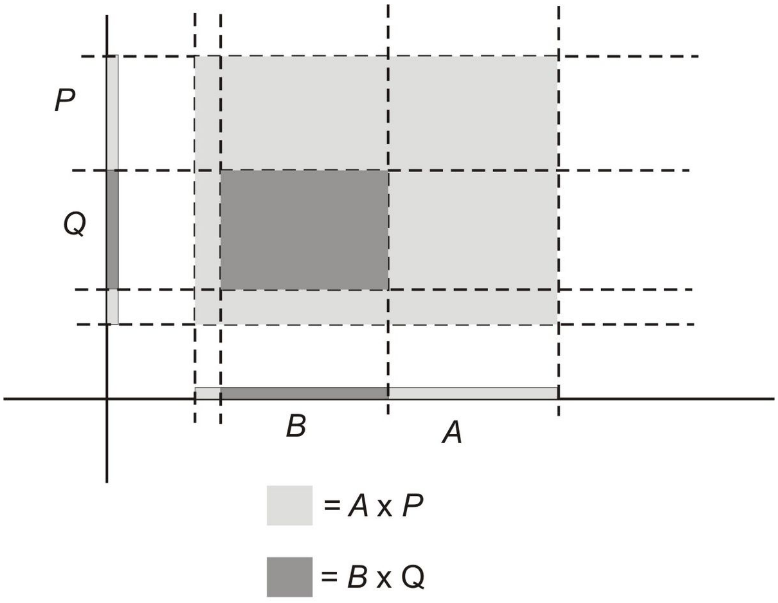
In addition, since $B \subset A$, then we must represent *B* as a set chosen from within the elements of *A*. Similarly, since $Q \subset P$, the elements of *Q* must lie within the elements of *P*.

When we add these components on to the diagram it looks like this:



The Cartesian Plane: Fig. 9b

Finally, when we represent the set $B \times Q$ as a rectangle whose limits are determined by the limits of *B* and *Q*, it is clear that this rectangle will lie within the rectangle representing $A \times P$:



The Cartesian Plane: Fig. 9c

So, the proposition $B \times Q \subset A \times P$ appears to be true.

Set Theory Exercise 5

Click link for Set Theory Exercise 5.

Previous topic:../../Introduction|Contents:Discrete Mathematics|Next topic:../../Functions and relations

References

[1] http://en.wikipedia.org/wiki/Boolean_algebra

Discrete Mathematics/Functions and relations

This article examines the concepts of the *function* and the *relation*.

A ***relation*** is any association between elements of one set, called the ***domain*** or (less formally) the *set of inputs*, and another set, called the ***range*** or *set of outputs*. Some people mistakenly refer to the range as the *codomain*, but as we will see, that really means the *set of all possible outputs*—even values that the relation does not actually use.

For example, if the *domain* is a set Fruits = {apples, oranges, bananas} and the *codomain* is a set Flavors = {sweetness, tartness, bitterness}, the flavors of these fruits form a relation: we might say that apples are related to (or associated with) **both** sweetness and tartness, while oranges are related to tartness only and bananas to sweetness only. (We might disagree somewhat, but that is irrelevant to the topic of this book.) Notice that "bitterness", although it is one of the possible Flavors (codomain), is not really used for any of these relationships; so it is not part of the *range* {sweetness, tartness}.

Another way of looking at this is to say that a relation is a *subset of ordered pairs* drawn from the *set of all possible ordered pairs* (of elements of two other sets, which we normally refer to as the *Cartesian product* of those sets). Formally, R is a relation if

$$R \subseteq \{(x, y) \mid x \in X, y \in Y\}$$

for the domain X and codomain Y.

Using the example above, we can write the relation in set notation: {(apples, sweetness), (apples, tartness), (oranges, tartness), (bananas, sweetness)}.

One important kind of relation is the *function*. A ***function*** is a relation that has **exactly one output** for every possible input **in the domain**. (Unlike the codomain, the domain does not necessarily have to include all possible objects of a given type. In fact, we sometimes intentionally use a *restricted domain* in order to satisfy some desirable property.) For example, the relation that we discussed above (flavors of fruits) is **not** a function, because it has two possible outputs for the input "apples": sweetness and tartness.

The main reason for not allowing multiple outputs with the same input is that it lets us apply the same function to different forms of the same thing without changing their equivalence. That is, if x = y, and f is a function with x (or y) in its domain, then f(x) = f(y). For example, z - 3 = 5 implies that z = 8 because f(x) = x + 3 is a function defined for all numbers x.

The converse, that f(x) = f(y) implies x = y, is not always true. When it is, f is called a **one-to-one** or **invertible function**.

Relations

In the above section dealing with functions and their properties, we noted the important property that all functions must have, namely that if a function does map a value from its domain to its co-domain, it must map this value to only one value in the co-domain.

Writing in set notation, if *a* is some fixed value:

$$|\{f(x)|x=a\}| \in \{0, 1\}$$

The literal reading of this statement is: the *cardinality* (number of elements) of the set of all values f(x), such that x=a for some fixed value a, is an element of the set {0, 1}. In other words, the number of *outputs* that a function f may have at any fixed *input* a is either zero (in which case it is *undefined* at that input) or one (in which case the output is unique).

However, when we consider the *relation*, we relax this constriction, and so a relation may map one value to more than one other value. In general, a relation is **any** subset of the Cartesian product of its domain and co-domain.

All functions, then, can be considered as relations also.

Notations

When we have the property that one value is related to another, we call this relation a *binary relation* and we write it as

$$x \, R \, y$$

where R is the relation.

For arrow diagrams and set notations, remember for relations we do not have the restriction that functions do and we can draw an arrow to represent the mappings, and for a set diagram, we need only write all the ordered pairs that the relation does take: again, by example

$$f = \{(0,0),(1,1),(1,-1),(2,2),(2,-2)\}$$

is a relation and not a function, since both 1 and 2 are mapped to two values, 1 and -1, and 2 and -2 respectively) example let A=2,3,5;B=4,6,9 then A*B=(2,4),(2,6),(2,9),(3,4),(3,6),(3,9),(5,4),(5,6),(5,9) Define a relation R=(2,4),(2,6),(3,6),(3,9)

Some simple examples

Let us examine some simple relations.

Say f is defined by

{(0,0),(1,1),(2,2),(3,3),(1,2),(2,3),(3,1),(2,1),(3,2),(1,3)}

This is a relation (not a function) since we can observe that 1 maps to 2 and 3, for instance.

Less-than, "<", is a relation also. Many numbers can be less than some other fixed number, so it cannot be a function.

Properties

When we are looking at relations, we can observe some special properties different relations can have.

Reflexive

A relation is *reflexive* if, we observe that for all values a:

a R a

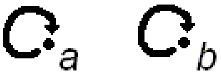
In other words, all values are related to themselves.

The relation of equality, "=" is reflexive. Observe that for, say, all numbers a (the domain is **R**):

$a = a$

so "=" is reflexive.

In a reflexive relation, we have arrows for all values in the domain pointing back to themselves:



Note that ≤ is also reflexive (a ≤ a for any a in **R**). On the other hand, the relation < is not (a < a is false for any a in **R**).

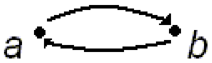
Symmetric

A relation is *symmetric* if, we observe that for all values a and b:

a R b implies b R a

The relation of equality again is symmetric. If x=y, we can also write that y=x also.

In a symmetric relation, for each arrow we have also an opposite arrow, i.e. there is either no arrow between x and y, or an arrow points from x to y and an arrow back from y to x:



Neither ≤ nor < is symmetric (2 ≤ 3 and 2 < 3 but not 3 ≤ 2 nor 3 < 2 is true).

Transitive

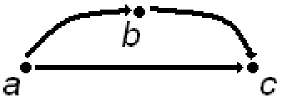
A relation is *transitive* if for all values *a*, *b*, *c*:

> *a* R *b* and *b* R *c* implies *a* R *c*

The relation *greater-than* ">" is transitive. If $x > y$, and $y > z$, then it is true that $x > z$. This becomes clearer when we write down what is happening into words. *x* is greater than *y* and *y* is greater than *z*. So *x* is greater than both *y* and *z*.

The relation *is-not-equal* "≠" is not transitive. If $x \neq y$ and $y \neq z$ then we might have $x = z$ or $x \neq z$ (for example $1 \neq 2$ and $2 \neq 3$ and $1 \neq 3$ but $0 \neq 1$ and $1 \neq 0$ and $0 = 0$).

In the arrow diagram, every arrow between two values *a* and *b*, and *b* and *c*, has an arrow going straight from *a* to *c*.



Antisymmetric

A relation is *antisymmetric* if we observe that for all values *a* and *b*:

> *a* R *b* and *b* R *a* implies that *a=b*

Notice that antisymmetric is not the same as "not symmetric."

Take the relation *greater than equals to*, "≥" If $x \geq y$, and $y \geq$ x, then *y* must be equal to *x*. a relation is anti-symmetric if and only if a∈A, (a,a)∈R

Trichotomy

A relation satisfies *trichotomy* if we observe that for all values *a* and *b* it holds true that: *a*R*b or b*R*a*

The relation *is-greater-or-equal* satisfies since, given 2 real numbers *a* and *b*, it is true that whether $a \geq b$ or $b \geq a$ (both if $a = b$).

Problem set

Given the above information, determine which relations are reflexive, transitive, symmetric, or antisymmetric on the following - there may be more than one characteristic. (Answers follow.) *x* R *y* if

1. x = y
2. x < y
3. $x^2 = y^2$
4. x ≤ y

Answers

1. Symmetric, Reflexive, Transitive and Antisymmetric
2. Transitive
3. Symmetric, Reflexive, Transitive and Antisymmetric ($x^2 = y^2$ is just a special case of equality, so all properties that apply to x = y also apply to this case)
4. Reflexive, Transitive and Antisymmetric (and satisfying Trichotomy)

Equivalence relations

We have seen that certain common relations such as "=", and congruence (which we will deal with in the next section) obey some of these rules above. The relations we will deal with are very important in discrete mathematics, and are known as *equivalence relations*. They essentially assert some kind of equality notion, or *equivalence*, hence the name.

Characteristics of equivalence relations

For a relation R to be an *equivalence relation*, it must have the following properties, viz. R must be:

- symmetric
- transitive
- reflexive

(A helpful mnemonic, S-T-R)

In the previous problem set you have shown equality, "=", to be reflexive, symmetric, and transitive. So "=" is an equivalence relation.

We denote an equivalence relation, in general, by $x \sim y$.

Example proof

Say we are asked to prove that "=" is an equivalence relation. We then proceed to prove each property above in turn (Often, the proof of transitivity is the hardest).

Reflexive

Clearly, it is true that *a* = *a* for all values a. So = is reflexive.

Symmetric

If *a* = *b*, it is also true that *b* = *a*. So = is symmetric

Transitive

If *a* = *b* and *b* = *c*, this says that *a* is the same as *b* which in turn is the same as *c*. So *a* is then the same as *c*, so *a* = *c*, and thus = is transitive.

Thus = is an equivalence relation.

```
any relation R on set A is said to be a transitive relation.
```

(a,b),(b,c)belongs to(a,c)belongs to R,where a,b,c belongs to a.

Partitions and equivalence classes

It is true that when we are dealing with relations, we may find that many values are related to one fixed value.

For example, when we look at the quality of *congruence*, which is that given some number *a*, a number congruent to *a* is one that has the same remainder or *modulus* when divided by some number *n*, as *a*, which we write

a ≡ b (mod n)

and is the same as writing

b = *a*+*kn* for some integer k.

(We will look into congruences in further detail later, but a simple examination or understanding of this idea will be interesting in its application to equivalence relations)

For example, 2 ≡ 0 (mod 2), since the remainder on dividing 2 by 2 is in fact 0, as is the remainder on dividing 0 by 2.

We can show that congruence is an equivalence relation (This is left as an exercise, below **Hint** use the equivalent form of congruence as described above).

However, what is more interesting is that we can group all numbers that are equivalent to each other.

With the relation congruence *modulo* 2 (which is using n=2, as above), or more formally:

x ~ y if and only if x ≡ y (mod 2)

we can group all numbers that are equivalent to each other. Observe:

$$0 \equiv 2 \equiv 4 \equiv \ldots \pmod 2$$
$$1 \equiv 3 \equiv 5 \equiv \ldots \pmod 2$$

This first equation above tells us all the *even* numbers are equivalent to each other under ~, and all the *odd* numbers under ~.

We can write this in set notation. However, we have a special notation. We write:

[0]={0,2,4,...}

[1]={1,3,5,...}

and we call these two sets *equivalence classes*.

All elements in an equivalence class by definition are equivalent to each other, and thus note that we do not need to include [2], since 2 ~ 0.

We call the act of doing this 'grouping' with respect to some equivalence relation *partitioning* (or further and explicitly *partitioning a set S into equivalence classes under a relation* ~). Above, we have partitioned **Z** into equivalence classes [0] and [1], under the relation of congruence modulo 2.

Problem set

Given the above, answer the following questions on equivalence relations (Answers follow to even numbered questions)

1. Prove that congruence is an equivalence relation as before (See hint above).
2. Partition {x | 1 ≤ x ≤ 9} into equivalence classes under the equivalence relation

$$x \sim y \text{ iff } x \equiv y \pmod 6$$

Answers

2. [0]={6}, [1]={1,7}, [2]={2,8}, [3]={3,9}, [4]={4}, [5]={5}

Partial orders

We also see that "≥" and "≤" obey some of the rules above. Are these special kinds of relations too, like equivalence relations? Yes, in fact, these relations are specific examples of another special kind of relation which we will describe in this section: the *partial order*.

As the name suggests, this relation gives some kind of ordering to numbers.

Characteristics of partial orders

For a relation R to be a partial order, it must have the following three properties, viz R must be:

- reflexive
- antisymmetric
- transitive

(A helpful mnemonic, R-A-T)

We denote a partial order, in general, by $x \preceq y$.

Example proof

Say we are asked to prove that "≤" is a partial order. We then proceed to prove each property above in turn (Often, the proof of transitivity is the hardest).

Reflexive

Clearly, it is true that $a \le a$ for all values a. So ≤ is reflexive.

Antisymmetric

If $a \le b$, and $b \le a$, then a *must* be equal to b. So ≤ is antisymmetric

Transitive

If $a \le b$ and $b \le c$, this says that a is less than b and c. So a is less than c, so $a \le c$, and thus ≤ is transitive.

Thus ≤ is a partial order.

Problem set

Given the above on partial orders, answer the following questions

1. Prove that divisibility, |, is a partial order (a | b means that a is a factor of b, i.e., on dividing b by a, no remainder results).
2. Prove the following set is a partial order: $(a, b) \preceq (c, d)$ implies $ab{\le}cd$ for a,b,c,d integers ranging from 0 to 5.

Answers

2. Simple proof; Formalization of the proof is an optional exercise.

Reflexivity: $(a, b) \preceq (a, b)$ since $ab{=}ab$.

Antisymmetric: $(a, b) \preceq (c, d)$ and $(c, d) \preceq (a, b)$ since $ab{\le}cd$ and $cd{\le}ab$ imply $ab{=}cd$.

Transitive: $(a, b) \preceq (c, d)$ and $(c, d) \preceq (e, f)$ implies $(a, b) \preceq (e, f)$ since $ab{\le}cd{\le}ef$ and thus $ab{\le}ef$

Posets

A partial order imparts some kind of "ordering" amongst elements of a set. For example, we only know that 2 ≥ 1 because of the partial ordering ≥.

We call a set A, ordered under a general partial ordering $\preceq$, a *partially ordered set*, or simply just *poset*, and write it (A, $\preceq$).

Terminology

There is some specific terminology that will help us understand and visualize the partial orders.

When we have a partial order $\preceq$, such that $a \preceq b$, we write $\prec$ to say that a $\preceq$ but $a \ne b$. We say in this instance that a *precedes* b, or a is a predecessor of b.

If (A, $\preceq$) is a poset, we say that *a* is an immediate predecessor of *b* (or *a* immediately precedes *b*) if there is no *x* in A such that $a \prec x \prec b$.

If we have the same poset, and we also have *a* and *b* in A, then we say *a* and *b* are *comparable* if $a \preceq b$ and $b \preceq a$. Otherwise they are *incomparable*.

Hasse diagrams

Hasse diagrams are special diagrams that enable us to visualize the structure of a partial ordering. They use some of the concepts in the previous section to draw the diagram.

A Hasse diagram of the poset (A, $\preceq$) is constructed by

- placing elements of A as points
- if *a* and *b* ∈ A, and *a* is an immediate predecessor of b, we draw a line from *a* to *b*
- if $a \prec b$, put the point for *a* lower than the point for *b*
- not drawing loops from *a* to *a* (this is assumed in a partial order because of reflexivity)

Operations on Relations

There are some useful operations one can perform on relations, which allow to express some of the above mentioned properties more briefly.

Inversion

Let R be a relation, then its inversion, R^{-1} is defined by

R^{-1} := {(a,b) | (b,a) in R}.

Concatenation

Let R be a relation between the sets A and B, S be a relation between B and C. We can concatenate these relations by defining

R • S := {(a,c) | (a,b) in R and (b,c) in S for some b out of B}

Diagonal of a Set

Let A be a set, then we define the diagonal (D) of A by

D(A) := {(a,a) | a in A}

Shorter Notations

Using above definitions, one can say (lets assume R is a relation between A and B):

R is *transitive* if and only if R • R is a subset of R.

R is *reflexive* if and only if D(A) is a subset of R.

R is *symmetric* if R^{-1} is a subset of R.

R is *antisymmetric* if and only if the intersection of R and R^{-1} is D(A).

R is *asymmetric* if and only if the intersection of D(A) and R is empty.

R is a *function* if and only if R^{-1} • R is a subset of D(B).

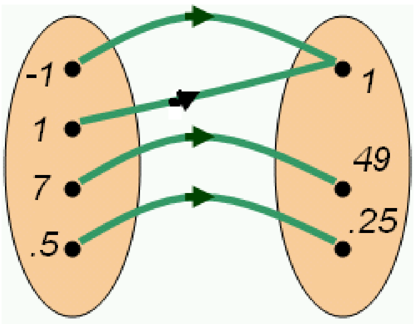
In this case it is a function A → B. Let's assume R meets the condition of being a function, then

R is *injective* if R • R^{-1} if a subset of D(A).

R is *surjective* if {b | (a,b) in R} = B.

Functions

A function is a relationship between two sets of numbers. We may think of this as a *mapping*; a function *maps* a number in one set to a number in another set. Notice that a function maps values to **one and only one** value. Two values in one set could map to one value, but one value **must never** map to two values: that would be a relation, *not* a function.



For example, if we write (define) a function as:

$$f(x) = x^2$$

then we say:

'f of x equals x squared'

and we have

$$f(-1) = 1$$
$$f(1) = 1$$
$$f(7) = 49$$
$$f(1/2) = 1/4$$
$$f(4) = 16$$

and so on.

This function f maps numbers to their squares.

Range, image, codomain

If D is a set, we can say

$$f(D) = \{f(x)|\ x \in D\}$$

which forms a new set, called the *range* of f. D is called the *domain* of f, and represents all values that f takes.

In general, the range of f is usually a subset of a larger set. This set is known as the *codomain* of a function. For example, with the function f(*x*)=cos *x*, the range of f is [-1,1], **but** the codomain is the set of real numbers.

Notations

When we have a function f, with domain D and range R, we write:

$$f : D \longrightarrow R$$

If we say that, for instance, *x* is mapped to x^2, we also can add

$$f : D \longrightarrow R;\ x \longmapsto x^2$$

Notice that we can have a function that maps a point (*x*,*y*) to a real number, or some other function of two variables -- we have a set of ordered pairs as the domain. Recall from set theory that this is defined by the *Cartesian product* - if we wish to represent a set of all real-valued ordered pairs we can take the Cartesian product of the real numbers with itself to obtain

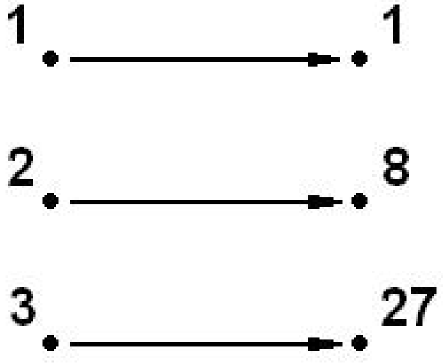
$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x,y)|\ x \text{ and } y \in \mathbb{R}\}\ .$$

When we have a set of *n*-tuples as part of the domain, we say that the function is *n*-ary (for numbers *n*=1,2 we say unary, and binary respectively).

Other function notation

Functions can be written as above, but we can also write them in two other ways. One way is to use an arrow diagram to represent the mappings between each element. We write the elements from the domain on one side, and the elements from the range on the other, and we draw arrows to show that an element from the domain is mapped to the range.

For example, for the function f(x)=x^3, the arrow diagram for the domain {1,2,3} would be:



Another way is to use set notation. If f(x)=y, we can write the function in terms of its mappings. This idea is best to show in an example.

Let us take the domain D={1,2,3}, and f(x)=x^2. Then, the range of f will be R={f(1),f(2),f(3)}={1,4,9}. Taking the Cartesian product of D and R we obtain F={(1,1),(2,4),(3,9)}.

So using set notation, a function can be expressed as the Cartesian product of its domain and range.

```
f(x)
```

This function is called *f*, and it takes a *variable x*. We substitute some value for *x* to get the second value, which is what the function maps x to.

This is incomplete and a draft, additional information is to be added

Previous topic: ../Functions and relations/ | Contents:Discrete Mathematics | Next topic: ../Number theory/

Discrete Mathematics/Number theory

Number theory is a large encompassing subject in its own right. Here we will examine the key concepts of number theory.

Introduction

Unlike real analysis and calculus which deals with the dense set of real numbers, number theory examines mathematics in discrete sets, such as **N** or **Z**. If you are unsure about sets, you may wish to revisit ../Set theory/.

Number Theory, the study of the integers, is one of the oldest and richest branches of mathematics. Its basic concepts are those of divisibility, prime numbers, and integer solutions to equations -- all very simple to understand, but immediately giving rise to some of the best known theorems and biggest unsolved problems in mathematics. The Theory of Numbers is also a very interdisciplinary subject. Ideas from combinatorics (the study of counting), algebra, and complex analysis all find their way in, and eventually become essential for understanding parts of number theory. Indeed, the greatest open problem in all mathematics, the Riemann Hypothesis, is deeply tied into Complex Analysis. But never fear, just start right into *Elementary Number Theory*, one of the warmest invitations to pure mathematics, and one of the most surprising areas of applied mathematics!

Divisibility

Note that in **R**, **Q**, and **C**, we can *divide* freely, except by zero. This property is often known as *closure* -- the quotient of two rationals is again a rational, etc.. However, if we move to performing mathematics purely in a set such as **Z**, we come into difficulty. This is because, in the integers, the result of a division of two integers might not be another integer. For example, we can of course divide 6 by 2 to get 3, but we *cannot* divide 6 by 5, because the fraction 6/5 is not in the set of integers.

However we can introduce a new relation where division **is** defined. We call this relation *divisibility*, and if $\frac{b}{a}$ is an integer, we say:

- a divides b
- a is a factor of b
- b is a multiple of a
- b is divisible by a

Formally, if there exists an integer q such that $b = qa$ then we say that a **divides** b and write $a \mid b$. If a does not divide b then we write $a \nmid b$:

Proposition. The following are basic consequences of this definition. Let a, b, and c be integers:

- (a) If a|b then a|(bc).
- (b) If a|b and b|c, then a|c.
- (c) If a|b and a|c, then for any integers x and y, a|(xb+yc) -- in other words a divides any *linear combination* of its multiples.
- (d) If both a|b and b|a, then a = b or a = -b.
- (e) If c is not 0, then a|b is equivalent to ca|cb.

Quotient and divisor theorem

For any integer n and any $k > 0$, there is a unique q and r such that:

$n = qk + r$ (with $0 \le r < k$)

We call q the *quotient*, r the *remainder*, and k the *divisor*.

It is probably easier to recognize this as division by the algebraic re-arrangement:

$n/k = q + r/k$ ($0 \le r/k < 1$)

Modular arithmetic

What can we say about the numbers that divide another? Pick the number 8 for example. What is the remainder on dividing 1 by 8? Using the division theorem above

0 = 8*0 + 0

1 = 8*0 + 1

2 = 8*0 + 2

:

8 = 8*1 + 0

9 = 8*1 + 1

10 = 8 * 1 + 2

:

and so on

We have a notation for the remainders, and can write the above equations as

0 mod 8 = 0

1 mod 8 = 1

2 mod 8 = 2

3 mod 8 = 3

4 mod 8 = 4

5 mod 8 = 5

6 mod 8 = 6

7 mod 8 = 7

8 mod 8 = 0

9 mod 8 = 1

10 mod 8 = 2

:

We can also write

$1 \equiv 1 \pmod 8$

$2 \equiv 2 \pmod 8$

$3 \equiv 3 \pmod 8$

$4 \equiv 4 \pmod 8$

$5 \equiv 5 \pmod 8$

$6 \equiv 6 \pmod 8$

$7 \equiv 7 \pmod 8$

$8 \equiv 0 \pmod 8$

$9 \equiv 1 \pmod 8$

$10 \equiv 2 \pmod 8$

:

These notations are all short for

$a = 8k+r$ for some integer k.

So $x \equiv 1 \pmod 8$, for example, is the same as saying

$x = 8k+1$

Observe that the remainder here, in comparing it with the division algorithm is 1. $x \equiv 1 \pmod 8$ asks what numbers have the remainder 1 on division by 8? Clearly the solutions are x=8×0+1, 8×1+1,... = 1, 9, ...

Often the entire set of remainders on dividing by n - which we say *modulo n* - are interesting to look at. We write this set $\mathbf{Z}_n$. Note that this set is finite. The remainder on dividing 9 by 8 is 1 - the same as dividing 1 by 8. So in a sense 9 is really "the same as" 1. In fact, the relation "≡"

$x \equiv y$ iff $x \bmod n = y \bmod n$.

is an equivalence relation. We call this relation *congruence*. Note that the equivalence classes defined by congruence are precisely the elements of $\mathbf{Z}_n$.

We can find some number a modulo n (or we say a congruent to n) by finding its decomposition using the division algorithm.

Addition, subtraction, and multiplication work in $\mathbf{Z}_n$ - for example 3 + 6 (mod 8) = 9 (mod 8) = 1 (mod 8). The numbers do look strange but they follow many normal properties such as commutativity and associativity.

If we have a number greater than n we often reduce it modulo n first - again using the division algorithm. For example if we want to find 11+3 mod 8, its often easier to calculate 3 + 3 (mod 8) rather than reducing 14 mod 8. A trick that's often used is that, say, if we have 6 + 7 (mod 8) we can use *negative* numbers instead so the problem becomes -2 + -1 = -3 = 5 (mod 8).

We often use the second notation when we want to look at equations involving numbers modulo some n. For example, we may want to find a number x such that

$3x \equiv 5 \pmod 8$

We can find solutions by trial substitution (going through all the numbers 0 through 7), but what if the moduli are very large? We will look at a more systematic solution later.

Note: we often say that we are working in $\mathbf{Z}_n$ and use equals signs throughout. Familiarize yourself with the three ways of writing modular equations and expressions.

Number Bases

Converting between various number bases is one of the most tedious processes in mathematics.

The numbers that are generally used in transactions are all in base-10. This means that there are 10 digits that are used to describe a number. These ten digits are {0,1,2,3,4,5,6,7,8,9}.

Similarly, base-4 has 4 digits {0,1,2,3} and base-2 has two digits {0,1}. Base two is sometimes referred to as Binary.

There are also bases greater than 10. For these bases, it is customary to use letters to represent digits greater than 10. An example is Base-16 (Hexadecimal). The digits used in this base are {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}.

In order to convert between number bases, it is critical that one knows how to divide numbers and find remainders.

To convert from decimal to another base one must simply start dividing by the value of the other base, then dividing the result of the first division and overlooking the remainder, and so on until the base is larger than the result (so the result of the division would be a zero). Then the number in the desired base is the remainders read from end to start.

The following shows how to convert a number (105) which is in base-10 into base-2.

Operation	Remainder
105 / 2 = 52	1
52 / 2 = 26	0
26 / 2 = 13	0
13 / 2 = 6	1
6 / 2 = 3	0
3 / 2 = 1	1
1 / 2 = 0	1

Answer : 1101001

After finishing this process, the remainders are taken and placed in a row (from bottom to top) after the final quotient (1101001, in this example) is shown as the base-2 equivalent of the number 105.

To sum up the process, simply take the original number in base 10, and divide that number repeatedly, keeping track of the remainders, until the quotient becomes less than the numerical value of the base.

This works when converting any number from base-10 to any base. If there are any letters in the base digits, then use the letters to replace any remainder greater than 9. For example, writing 11(of base-10) in base 14.

Operation	Remainder
11 / 14 = 0	B (=11)

Answer: B

As 11 is a single remainder, it is written as a single digit. Following the pattern {10=A, 11=B, 12=C...35=Z}, write it as B. If you were to write "11" as the answer, it would be wrong, as "11" Base-14 is equal to 15 in base-10!

In order to convert from a number in any base back to base ten, the following process should be used:

Take the number 3210 (in base-10). In the units place (10^0), there is a 0. In the tens place (10^1), there is a 1. In the hundreds place (10^2), there is a 2. In the thousands place (10^3), there is a 3.

The formula to find the value of the above number is:

$3\times10^3 + 2\times10^2 + 1\times10^1 + 0\times10^0 = 3000 + 200 + 10 + 0 =$ **3210**.

The process is similar when converting from any base to base-10. For example, take the number 3452 (in base-6). In the units place (6^0), there is a 2. In the sixths place (6^1) there is a 5. In the thirty-sixths place (6^2), there is a 4. In the 216th place (6^3), there is a 3.

The formula to find the value of the above number (in base-10) is:

$3\times6^3 + 4\times6^2 + 5\times6^1 + 2\times6^0 = 648 + 144 + 30 + 2 =$ **824**.

The value of 3452 (base-6) is **824** in base-10.

A more efficient algorithm is to add the left-most digit and multiply by the base, and repeat with the next digit and so on.

$((3 * 6 + 4) * 6 + 5) * 6 + 2 = 824$

The processes to convert between number bases may seem difficult at first, but become easy if one practices often.

Prime numbers

Prime numbers are the building blocks of the integers. A prime number is a positive integer greater than one that has only two divisors: 1, and the number itself. For example, 17 is prime because the only positive integers that divide evenly into it are 1 and 17. The number 6 is not a prime since more than two divsors 1, 2, 3, 6 divide 6. Also, note that 1 is not a prime since 1 has only one divisor.

Some prime numbers

The prime numbers as a sequence begin

2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Euclid's Proof that There are Infinitely Many Primes

The Greek mathematician Euclid gave the following elegant proof that there are an infinite number of primes. It relies on the fact that all non-prime numbers --- composites --- have a unique factorization into primes.

Euclid's proof works by contradiction: we will assume that there are a finite number of primes, and show that we can derive a logically contradictory fact.

So here we go. First, we assume that that there are a finite number of primes:

$p_1, p_2, \cdots, p_n$

Now consider the number M defined as follows:

$M = 1 + p_1 * p_2 * ... * p_n$

There are two important --- and ultimately contradictory --- facts about the number M:

1. It cannot be prime because p_n is the biggest prime (by our initial assumption), and M is clearly bigger than p_n. Thus, there must be some prime p that divides M.
2. It is not divisible by any of the numbers $p_1, p_2, ..., p_n$. Consider what would happen if you tried to divide M by any of the primes in the list $p_1, p_2, ... , p_n$. From the definition of M, you can tell that you would end up with a remainder of 1. That means that p --- the prime that divides M --- must be bigger than any of $p_1, ..., p_n$.

Thus, we have shown that M is divisible by a prime p that is not on the finite list of all prime. And so there must be an infinite number of primes.

These two facts imply that M must be divisible by a prime number bigger than p_n. Thus, there cannot be a biggest prime.

Note that this proof does not provide us with a direct way to generate arbitrarily large primes, although it always generates a number which is divisible by a new prime. Suppose we know only one prime: 2. So, our list of primes is simply p_1=2. Then, in the notation of the proof, M=1+2=3. We note that M is prime, so we add 3 to the list. Now, M = 1 +2 *3 = 7. Again, 7 is prime. So we add it to the list. Now, M = 1+2*3*7 = 43: again prime. Continuing in this way one more time, we calculate M = 1+2*3*7*43 = 1807 =13*139. So we see that M is not prime.

Viewed another way: note that while 1+2, 1+2*3, 1+2*3*5, 1+2*3*5*7, and 1+2*3*5*7*11 are prime, 1+2*3*5*7*11*13=30031=59*509 is not.

Testing for primality

There are a number of simple and sophisticated primality tests. We will consider some simple tests here. In upper-level courses we will consider some faster and more sophisticated methods to test whether a number is prime.

Inspection

The most immediate and simple test to eliminate a number n as a prime is to inspect the units digit or the last digit of a number.

If the number n ends in an even number 0, 2, 4, 6, 8 we can show that number n cannot be a prime. For example, take n = 87536 = 8753(10) + 6. Since 10 is divisible by 2 and 6 is divisible by 2 then 87536 must be divisible by 2. In general, any even number can be expressed in the form n = a*10 + b, where b = 0, 2, 4, 6, 8. Since 10 is divisible by 2 and b is divisible by 2 then n = a*10 + b is divisible by 2. Consequently, any number n which ends in an even number such as 7777732 or 8896 is divisible by 2 so n is not a prime.

In a similar type of argument, if a number n ends in a 5 we can show the number n cannot be a prime. If the last digit of n, call it b, is a 5 we can express n in the form n = a*10 + b, where b = 5. Since 10 is divisible by 5 and b = 5 is divisible by 5 then n = a*10 + b is divisible by 5. Hence, any number n which ends in a 5 such as 93475 is divisible by 5 so n is not a prime.

Thus, if a number greater than 5 is a prime it must end with either a 1, 3, 7, or 9. Note that this does not mean all numbers that end in a 1, 3, 7, or 9 are primes. For example, while the numbers 11, 23, 37, 59 are primes, the numbers 21 = 3*7, 33 = 3*11, 27 = 3*9, 39 = 3*13 are not primes. Consequently, if a number ends in a 1, 3, 7, or 9 we have to test further.

Trial Division Method

To test if a number n that ends in a 1, 3, 7, or 9 is prime, we could simply try the smallest prime number and try to divide it in n. If that doesn't divide, we would take the next largest prime number and try again etc. Certainly, if we took all primes numbers in this manner that were less than n and we could not divide n then we would be justified in saying n is prime. However, it can be shown that you don't have to take all primes smaller than n to test if n is prime. We can stop earlier by using the Trial Division Method.

The justification of the Trial Division Method is if a number n has no divisors less than or equal to $\sqrt{n}$ then n must be a prime. We can show this by contradiction. Let us assume n has no divisors less than or equal to $\sqrt{n}$. If n is not a prime, there must be two numbers a and b such that $a * b = n$. In particular, by our assumption $\sqrt{n} < a$ and $\sqrt{n} < b$. But then $n = \sqrt{n}\sqrt{n} < a * b = n$. Since a number can not be greater than itself the number n must be a prime.

Trial Division Method is a method of primality testing that involves taking a number n and then sequentially dividing it by primes up to $\sqrt{n}$.

For example, is 113 prime? $\sqrt{113}$ is approximately 10.63... We only need to test whether 2, 3, 5, 7 divide 113 cleanly (leave no remainder, i.e., the quotient is an integer).

113/2 is not an integer since the last digit is not even.

113/3 (=37.666...) is not an integer.

113/5 is not an integer since the last digit does not end in a 0 or 5.

113/7 (=16.142857...) is not an integer.

So we need not look at any more primes such as 11, 13, 17 etc. less than 113 to test, since 2, 3, 5, 7 does not divide 113 cleanly, 113 is prime.

Notice that after rejecting 2 and 3 as a divisor, we next considered the next prime number 5 and not the next number 4. We know not to consider 4 because we know 2 does not divide 113. If 2 cannot divide 113 then certainly 4 cannot because if 4 divided 113 and since 2 divides 4 then 2 would divide 113. So we only use the next cheapest available prime to test not the next consecutive number.

If we test 91 we get,

> 91/2 is not an integer since that last digit is not even.
>
> 91/3= (30.333) is not an integer.
>
> 91/5= is not an integer since the last digit does not end in a 0 or 5.
>
> 91/7=13 is an integer

So we know since 7 divides 91, 91 is not a prime.

Trial division is normally only used for relatively small numbers due to its inefficiency. However this technique has the two advantages that firstly once we have tested a number we know for sure that it is prime and secondly if a number is not prime it also gives us the number's factors.

To obtain a few small primes, it may be best to use the Sieve of Eratosthenes than to test each number sequentially using trial division. The Sieve of Eratosthenes method is basically a process of finding primes by elimination. We start by taking a list of consecutive numbers say 1 to 100. Cross out the number 1 because the number is not prime. Take the next least uncrossed off number which is 2 and circle it. Now cross out all multiples of 2 on the list. Next take the next least uncircled number which is 3. Circle the number 3 and cross out all multiples of 3. The next least uncircled number should be 5 since 4 is a multiple of 2 and should have been crossed off. Circle the number 5 and cross out all multiples of 5. The next least uncircled number should be a 7 since 6 is a multiple of 2. Circle the 7 and mark off all multiples of 7. Now the next uncrossed off number should be 11 since 8,9,10 is a multiple of 2, 3, and 2. If we continue in this manner what is left is the circled numbers which are primes. But notice we can actually stop now and circle all the unmarked numbers after crossing off multiples of 7 because of the result that since $\sqrt{100} = 10$ any number less than 100 which is not prime must be divisible by 2, 3, 5, or 7.

The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic is an important theorem relating to the factorization of numbers. The theorem basically states that every positive integer can be written as the product of prime numbers in a unique way (ignoring reordering the product of prime numbers).

In particular, **The Fundamental Theorem of Arithmetic** means any number such as 1,943,032,663 is either a prime or can be factored into a product of primes. If a number such as 1,943,032,663 can be factored into primes such as 11×13×17×19×23×31×59 it is futile to try to find another different combination of prime numbers that will also give you the same number.

To make the theorem work even for the number 1, we think of 1 as being the product of zero prime numbers.

More formally,

> For all $n \in \mathbf{N}$
>
> > $n = p_1 p_2 p_3 \cdots$
>
> where the p_i are all prime numbers, and can be repeated.

Here are some examples.

> $4 = 2 \times 2 = 2^2$
>
> $12 = 2 \times 2 \times 3 = 2^2 \times 3$
>
> $11 = 11.$

A proof of the Fundamental Theorem of Arithmetic will be given after Bezout's identity has been established.

LCM and GCD

Two characteristics we can determine between two numbers based on their factorizations are the *lowest common multiple*, the *LCM* and *greatest common divisor*, the *GCD* (also *greatest common factor*, *GCF*)

LCM

The lowest common multiple, or the least common multiple, for two numbers a and b is the smallest number designated by LCM(a,b) that is divisible by both the number a and the number b. We can find LCM(a,b) by finding the prime factorization of a and b and choosing the maximum power for each prime factor.

In another words, if the number a factors to $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, and the number b factors to $p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, then LCM(a,b) = $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ where $\gamma_i = Maximum(\alpha_i, \beta_i)$ for *i* = *1 to n.*
An example, let us see the process on how we find lowest common multiple for 5500 and 450 which happens to be 49500. First, we find the prime factorization for 5500 and 450 which is

5500=2^2 5^3 11

450=2 3 ^{2} 5^2

Notice the different primes we came up for both the number 5500 and the number 450 are 2, 3, 5, and 11. Now let us express 5500 and 450 completely in a product of these primes raised to the appropriate power.

5500=2^2 5^3 11 = 2^2 3^0 5^3 11^1
450=2 3 2 5^2 = 2^1 3^2 5^2 11^0

The LCM(5500,450) is going to be in the form $2_?$ $3^?$ $5^?$ $11^?$. All we now have to do is find what the powers of each individual prime will be.

So now we compare the power of each prime for 5500 and 450. Let us consider the powers of the first prime 2. In the number 5500, the prime 2 is raised to the second power and in the number 450, prime 2 is raised to the first power. Since the maximum between 2 and 1 for the power of the prime 2 is 2, we use 2 for the power of the prime 2.

Now let us consider the powers of the prime 3. In the number 5500, the prime 3 is raised to the zero power and in the number 450 the prime 3 is raised to the second power. Since the maximum between 0 and 2 for the power of the prime 3 is 2, we use 2 for the power of the prime 3.

Similarly, let us consider the powers of the next prime 5. In the number 5500, the prime 5 is raised to the third power and in the number 450 the prime 5 is raised to the second power. Since the maximum between 3 and 2 for the power of the prime 5 is 3, we use 3 for the power of the prime 5.

Finally, let us consider the powers of the prime 11, the last prime on our list. In the number 5500, the prime 11 is raised to the first power and in the number 450 the prime 11 is raised to the zero power. Since the maximum between 1 and 0 for the power of the prime 11 is 1, we use 1 for the power of the last prime 11.

Consequently, the product of our results is LCM(5500,450)=2^2 3^2 5^3 11^1 = 49500.

GCD

The greatest common divisor for two numbers a and b is the biggest number designated by GCD(a,b) that divides both the number a and the number b. In a similar process to finding LCM(a,b), we can find GCD(a,b) by finding the prime factorization of a and b but choosing the minimum power for each prime factor instead.

In other words, if the number a factors to $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, and the number b factors to $p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, then GCD(a,b) = $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ where $\gamma_i = Minimum(\alpha_i, \beta_i)$ for *i* = *1 to n.*
An example, let us see the process on how we find the greatest common divisor for 5500 and 450 which happens to be 50. First, we find the prime factorization for 5500 and 450 which is

5500=2^2 5^3 11

$450=2\ 3\ ^2\ 5^2$

Notice the different primes we came up for both the number 5500 and the number 450 are 2, 3, 5, and 11. Now let us express 5500 and 450 completely in a product of these primes raised to the appropriate power.

$5500=2^2\ 5^3\ 11 = 2^2\ 3^0\ 5^3\ 11^1$

$450=2\ 3_2\ 5^2 = 2^1\ 3^2\ 5^2\ 11^0$

The GCD(5500,450) is going to be in the form $2_?\ 3^?\ 5^?\ 11^?$. All we now have to do is find what the powers of each individual prime will be.

So now we compare the power of each prime for 5500 and 450. Let us consider the powers of the first prime 2. In the number 5500, the prime 2 is raised to the second power and in the number 450, prime 2 is raised to the first power. Since the minimum between 2 and 1 for the power of the prime 2 is 2, we use 1 for the power of the prime 2.

Now let us consider the powers of the prime 3. In the number 5500, the prime 3 is raised to the zero power and in the number 450 the prime 3 is raised to the second power. Since the minimum between 0 and 2 for the power of the prime 3 is 0, we use 0 for the power of the prime 3.

Similarly, let us consider the powers of the next prime 5. In the number 5500, the prime 5 is raised to the third power and in the number 450 the prime 5 is raised to the second power. Since the minimum between 3 and 2 for the power of the prime 5 is 2, we use 2 for the power of the prime 5.

Finally, let us consider the powers of the prime 11, the last prime on our list. In the number 5500, the prime 11 is raised to the first power and in the number 450 the prime 11 is raised to the zero power. Since the minimum between 1 and 0 for the power of the prime 11 is 0, we use 0 for the power of the last prime 11.

Consequently, the product of our results is GCD(5500,450)=$2^1\ 3^0\ 5^2\ 11^0 = 50$.

Properties

- gcd(*a*,*b*)=gcd(*b*,*a*)
- gcd(*a*,*b*) = gcd(*b*,*q*), where *q* is the remainder of a divided by b
- gcd(*a*/*d*, *b*/*d*)=1, where *d* is gcd(*a*,*b*)

The Euclidean algorithm

The Euclidean algorithm is such that we can find the gcd of two numbers without finding the factorization*. The Euclidean algorithm consists of only addition and multiplication, and uses the above properties of gcd as its basis.

* Factorization is a "hard" process, that is, to factor a number takes a long time depending on the length of the number. This is why later, when you need to find the gcd of a pair of numbers, you will most likely *never* factorize the numbers and use the properties of the primes but will use the Euclidean algorithm instead.

An example

We will see how this works by calculating gcd(44,458)

First, divide 458 by 44 and obtain the remainder:

$458 = 44 \times 10 + 18$

Now suppose that a number is a common divisor of 458 and 44. Then it must also be a divisor of 18. To see this, rearrange the above equation to:

$458 - 44\times10 =18$

When this equation is divided by a common divisor of 44 and 458, an integer is obtained on the left, and so must also be obtained on the right. This, by definition, means that the number is also a divisor of 18. By the same reasoning, any common divisor of 18 and 44 is also a divisor of 458. Since all of the common divisors of 458 and 44 are equal to common divisors of 44 and 18, then in particular the greatest common divisors are equal. So we have gcd(458,44)=gcd(44,18)

The next step in the algorithm is to divide 44 by 18 and find the remainder.

$44 = 18 \times k + r$

$44 = 18 \times 2 + 8$

Repeat this process; keep dividing the previous divisor by the previous remainder:

$18 = 8 \times 2 + 2$

$8 = 2 \times 4 + 0$

Our gcd is the last remainder before the zero, in this case, 2. This is because the reasoning that proved gcd(458,44)=gcd(44,18) applies at every step, so gcd(458,44)=gcd(44,18)=gcd(18,8)=gcd(8,2)=gcd(2,0)=2.

The Matrix Method

We can construct a matrix that provides an alternative method for calculating the greatest common divisor. In its general form, the matrix is

$$\begin{bmatrix} 1 & 0 & b \\ 0 & 1 & a \end{bmatrix}$$

Recall that one way to write the gcd of two numbers is as an **integral linear combination**. If we are finding the gcd, for example, we could represent it as $as + bt$, where a and b are the two numbers we are comparing, and s and t are integers. We also know that $b = aq + r$ where r is the remainder upon division of b by a. After we subtract row 2 from row 1, we get

$$\begin{bmatrix} 1 & -q_1 & r_1 \\ 0 & 1 & a \end{bmatrix}$$

If r_2 is nonzero, we must continue the process; this time, subtracting row 1 from row 2. We continue this process until one of the *r's* has been reduced as far as possible. We now have our gcd. The numbers that are in that row, where the 1 and the 0 used to be, represent *t* and *s*, respectively.

Let us now look at a computational example.

$$\begin{bmatrix} 1 & 0 & 99 \\ 0 & 1 & 7 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 & 99 \\ 0 & 14 & 98 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -14 & 1 \\ 0 & 14 & 98 \end{bmatrix}$$

We see that it would be trivial at this point to go any further; we would just end up with row-2 containing a zero where *a* used to be. So we look at row-1 and remember that the *1* represents our remainder, 1(=t) multiplies *b* and -14(=s) multiplies *a* such that

$$1 = 99 \times 1 + -14 \times 7$$

This can be checked by the Euclidean algorithm that gcd(7,99)=1.

The extended Euclidean algorithm

What happens if we try and reverse the process of the Euclidean algorithm by substituting back? Back-substitution is rather tedious and prone to error, so here is a faster method.

Draw up a table with four columns, label these from left to right *q*, *r*, *u*, *v*. For convenience label a column *i* representing the step we're currently up to. Place *a* and *b* with the greater of these on top in the column *r*, and place 1s and 0s accordingly:

i	q	r	u	v
-1	.	b	0	1
0	.	a	1	0

Now iterate downwards by taking the quotient of *b*/*a* and putting it in the next space in the *q* column, then of *b*-*aq* in the *r* column.

To update *u* and *v*, take

$u_i = u_{i-2} - u_{i-1} q_i$

$v_i = v_{i-2} - v_{i-1} q_i$

Indeed, you are looking for *u* and *v* such that a*u* + b*v* = gcd (a,b). At some point, gcd (a,b) is in fact the remainder at the ith stage, so you might as well compute u_i and v_i such that $\mathrm{a}u_i + \mathrm{b}v_i = \mathrm{r}_i$, at EACH stage.

Deriving the recurrences found above results from these three equations (the second equation is Euclid's algorithm's basic property, the other two are constraints we set to attain our desired goal):

$\mathrm{a}u_{i-1} + \mathrm{b}v_{i-1} = \mathrm{r}_{i-1}$

$\mathrm{r}_{i-2} = \mathrm{q}_i \mathrm{r}_{i-1} + \mathrm{r}_i$

$\mathrm{a}u_i + \mathrm{b}v_i = \mathrm{r}_i$

The trick is to then appropriately express r_{i-2}.

Stop writing when you obtain a 0 in the *r* column.

Finding then, gcd(450,44) (this is the same as gcd(44,450))

i	q	r	u	v
-1	.	450	0	1
0	.	44	1	0
1	10	10	-10	1
2	4	4	41	-4
3	2	**2**	-92	9
4	2	0	$-$	$-$

The bold number is the gcd. Observe (9)×450+(-92)×44=2 Clearly these *u* and *v* are very special. What can we say about the general case?

Bezout's identity

In the above case we have 9×450+(-92)×44=gcd(450,44). So the greatest common divisor of 450 and 44 can be written as a linear combination of 450 and 44 with integer coefficients. This turns out to be true of any pair of integers. This result is known as "Bezout's Identity" and can be stated as follows:

> For any pair of nonzero integers, *a* and *b*, there exists integers *u* and *v* such that
>
> *au+bv=gcd(a,b)*

Proof

> If *a* and *b* are any pair of integers, not both 0, then clearly there exist integers *u* and *v* such that *au+bv* is positive (just match the signs of *u* and *v* to those of *a* and *b*, respectivly, for instance), and for all integer *u* and *v*, *au+bv* is also an integer (because the integers are closed under addition and multiplication). So there is a non-empty set of positive integers consisting of numbers of the form *au+bv*; call it S. Since S is a non-empty set of positive integers, it must have a smallest element (this is the so called Well-ordering principle). Call this number *d*. The claim is that $d = gcd(a, b)$. Since *d* belongs to S, then
>
> (1) $d = ua + vb$
>
> for suitable *u* and *v*. Let *n* be any positive common divisor of *a* and *b*. Since *n* divides the right side of (1), it also divides d. So $d = qn$ for some integer $q \geq 1$. So any common divisor of *a* and *b* is less than or equal to *d*. Therefore, if *d* is a common divisor of *a* and *b*, it is the greatest one. It only remains to show that *d* is in fact a common divisor.

To prove this, it will be shown that any element of S is divisible by *d*. This will prove that *d* is a common divisor of *a* and *b* because *a* and *b* are both elements of S (because *a* = 1×a + 0×b and*b* = 0×a + 1×b). Let *t* be any element of S. Then, by the division algorithm

$$t = qd + r$$

for some $0 \leq r < d$. If *r* is not 0, then it is in S. This is because *d* and *t* are in S, so

$$r = t - qd = (u_1a + v_1b) - q(u_2a + v_2b) = (u_1 - qu_2)a + (v_1 - qv_2)b = u'a + v'b$$

But, since $r < d$ and *d* is the least element of S, this is impossible. The only other possibility is that *r=0*. Therefore any element, *t*, of S is divisible by *d*. Since this includes both *a* and *b*, *d* is a common divisor. Combining this with the previous result establishes Bezout's Identity.

The numbers *u* and *v* can either be obtained using the tabular methods or backsubstitution in the Euclidean Algorithm.

Proof of the Fundamental Theorem of Arithmetic

One use of Bezout's identity is in a proof of the Fundamental Theorem of Arithmetic. Before this is proven, two other results are needed: Lemma 1: If a prime number, *p*, divides a product of two integers, ab , then it must divide *a* or *b* (or both).

Proof: If *p* divides both *a* and *b*, there is nothing to prove. Assume *p* does not divide *a*. If it can be proven under that assumption that *p* does divide *b*, the lemma will be proven.

Since *p* does not divide *a*, then *gcd(a,p)*=1 (because the only divisors of *p* are 1 and *p*, but *p* is not a common divisor). Therefore, by Bezout's Identity, there exist integers *u* and *v* such that

$$1 = ua + vp$$

Multiply this equation by *b* to obtain:

$$b = uab + vbp$$

p divides both terms on the right hand side and, therefore, divides the left hand side. Hence, *p* divides *b*, as was to be shown.

Lemma 2: If a prime number, *p*, divides a product of integers, $a_1a_2...a_n$, then it must divide at least one of the factors.

Proof: The proof is by induction on *n*, the number of factors. The statement is true for n=2, by Lemma 1. Assume the statement is true for *n=k* and consider a product of *k*+1 factors. If *p* divides more than one of the factors, once again there is nothing to prove. Assume that *p* does not divide any of the factors $a_1, a_2, ...a_k$. It will be shown that *p* must divide a_{k+1} . Since the statement is true for n=k, then since *p* does not divide any of the factors in $a_1a_2...a_k$, it must not divive the product (by Contrapositive). Let $a_1a_2...a_k = b$. Then $a_1a_2...a_ka_{k+1} = ba_{k+1}$. The conclusion then follows by Lemma 1.

Fundamental Theorem of Arithmetic:Any positive integer, *n*, can be expressed as a product of primes. This product is unique up to the order in which the terms appear.

Proof: The proof of the first part of the theorem is by induction on *n*. If *n*=1, it is the product of 0 primes. Assume all positive integers less than *n* can be expressed as a product of primes. If *n* is prime, then it is the product of 1 prime. Assume *n* is not prime or 1. Then $n = ab$,for some positive integers *a* and *b* both less than *n*. Since *a* and *b* are both less than *n*, they can be written as a product of primes by the induciton hypothesis. Combining these products gives *n* as a product of primes as required.

Now to prove the second part. Assume there are two prime factorizations of *n*,

$$n = p_1p_2...p_k = q_1q_2...q_s$$

p_1 divides the left side and so must also divide the right side. By Lemma 2, this means that p_1 must divide one of the q_i. But these are all prime, so the only way p_1 can divide q_i is if $p_1 = q_i$ for some *i*. Canceling p_1 from both sides of the equation forms another equation of the same form. So it can likewise be proven that $p_2 = q_i$ for some other *i*, and so on until all the factors on the left are exhausted. After this, there must not be any factors remaining on the right side since it must equal 1. This proves that any two prime factorizations consist of the same prime factors, as was to be shown.

Solving linear modular equations - back to Bezout

Bezout's identity above provides us with the key to solving equations in the form

$ax \equiv b \pmod{m}$

Coprime case - gcd(*a*, *m*) is 1

Consider the case where

$ax \equiv b \pmod{m}$

but with gcd(*a*, *m*)=1

Because of Bezout's identity

$1 = au+mv$

When we calculate *u*, this number is special.

Say if we have the equation

$4x=11 \pmod{21}$

4 and 21 are coprime since gcd(4,21)=1. Now 1=4*16+(-3)*(21). Our *u* in this case is 16. Observe now that 4*16=64. 64 (mod 21) = 1. This number *u* is very special - it is known as the *multiplicative inverse*. It is the number *u* on multiplication by *a* gives 1 mod *m*. Bezout's identity on calculating gcd(*a*, *m*) will always give you the multiplicative inverse of *a* modulo *m*. The multiplicative inverse of *a* is often written a^{-1} but note that this does ***not*** mean 1/*a* since we have seen in the first sections that we can not always divide in the integers.

Note that in $\mathbf{Z}_p$ there is one number *without* a multiplicative inverse - 0. It may be useful to exclude 0 when considering modular arithmetic, so instead of having to say $\mathbf{Z}_p\backslash\{0\}$ all the time, we merely write $\mathbf{Z}_p^*$.

Now since we have the magic multiplicative inverse, our problem becomes relatively easy to solve. $4^{-1}=16$ in $\mathbf{Z}_{21}$ and now, on multiplying throughout by 16

$x = 11 \times 16 \pmod{21}$

(since 4×16=1 because 16 is 4's multiplicative inverse mod 21). 11×16=176 and using a calculator or using the division theorem we obtain

$x = 8 \pmod{21}$

which is our solution! Verify - 8×4 = 32 = 11 (mod 21).

The general case

Consider the general case where

$ax \equiv b \pmod{m}$

with no restrictions on a, b and m.

Firstly we calculate

gcd

gcd(a, m) again to obtain d. Now d is a *divisor* since the d in gc$d$ means greatest common divisor. So we can now divide a and m - but what about b? Since we have calculated the gcd of a and m **but not *b*** we have no guarantees that d will divide b. This then becomes a condition that the equation has no solution.

Now we have reduced the problem to the previous coprime case because gcd(a/d, m/d)=1 with d as above. However we do not have 1 solution any more - this is true because we have reduced the solution to being $x = c \pmod{m/d}$ and we must bring the solution back mod m. This will be come clearer in the examples.

Let's work through some examples.

Example 1. Solve $4x \equiv 3 \pmod{20}$. Firstly, gcd(4, 20) = 4. 4 does not divide 3 and we have no solution.

Example 2. Solve $9x \equiv 6 \pmod{15}$. gcd(9, 15) = 3 and 3 does divide 6 and we have 3 solutions.

Now, divide through by 3 to obtain

$3x \equiv 2 \pmod{5}$

gcd(3, 5) = 1 = 3 × 2 + -1 × 5 So the inverse of 3 mod 5 is 2. Now we obtain the solution

$x \equiv 4 \pmod{5}$

Now in $\mathbf{Z}_{15}$ we must obtain the two extra solutions 9 and 14 mod 15 - 9 mod 5 = 4 and 14 mod 5 = 4.

Generally we can say that if we have the solution to the reduced equation x, the general solution is $x+(m/d)k$ for $k=\{0, 1, .., d-1\}$.

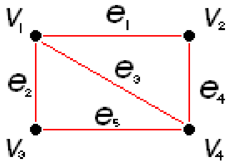
Discrete Mathematics/Graph theory

A *graph* is a mathematical way of representing the concept of a "network".

Introduction

A network has points, connected by lines. In a graph, we have special names for these. We call these points *vertices* (sometimes also called nodes), and the lines, *edges*.

Here is an example graph. The edges are red, the vertices, black.



In the graph, v_1, v_2, v_3, v_4 are vertices, and e_1, e_2, e_3, e_4, e_5 are edges.

Definitions of graph

There are several roughly equivalent definitions of a **graph**. Most commonly, a graph G is defined as an ordered pair $G = (V, E)$, where $V = \{v_1, \ldots, v_n\}$ is called the graph's **vertex-set** and $E = \{e_1, \ldots, e_m\} \subset \{\{x, y\} | x, y \in V\}$ is called the graph's **edge-set**. Given a graph G , we often denote the vertex--set by $V(G)$ and the edge--set by $E(G)$. To visualize a graph as described above, we draw n dots corresponding to vertices $v_1, \cdots, v_n$. Then, for all $i, j \in \{1, \ldots, n\}$ we draw a line between the dots corresponding to vertices v_i, v_j if and only if there exists an edge $\{v_i, v_j\} \in E$. Note that the placement of the dots is generally unimportant; many different pictures can represent the same graph.

Alternately, using the graph above as a guide, we can define a graph as an ordered triple $G = (V, E, f)$:

- a set of vertices, commonly called V
- a set of edges, commonly called E
- a relation $f : E \longrightarrow \{\{x, y\} | x, y \in V\}$ that maps to each edge a set of *endpoints*, known as the *edge-endpoint relation*. We say an edge $e \in E$ is **incident** to a vertex $v \in V$ iff $v \in f(e)$.

In the above example,

- V={v_1, v_2, v_3, v_4}
- E={e_1, e_2, e_3, e_4, e_5}
- f such that e_1 maps to {v_1, v_2}, e_2 maps to {v_1, v_3}, e_3 maps to {v_1, v_4}, e_4 maps to {v_2, v_4}, and e_5 maps to {v_3, v_4}.

If f is not injective — that is, if $\exists e, e' \in E$ such that $e \neq e', f(e) = f(e')$ — then we say that G is a **multigraph** and we call any such edges $e, e' \in E$ *multiple edges*. Further, we call edges $e \in E$ such that $|f(e)| = 1$ **loops**. Graphs without multiple edges or loops are known as **simple graphs**.

Graphs can, conceivably, be infinite as well, and thus we place no bounds on the sets V and E. We will not look at infinite graphs here.

Directions, Weights, and Flows

We define a **directed graph** as a graph such that f maps into the set of ordered pairs $\{(x,y)|x,y\in V\}$ rather than into the family of two-element sets $\{\{x,y\}|x,y\in V\}$. We can think of an edge $e\in E$ such that $f(e)=(x,y)$ as 'pointing' from x to y. As such we would say that x is the *tail* of edge e and that y is the *head*. This is one of the vagaries of graph theory notation, though. We could just as easily think of x as the head and y as the tail. To represent a directed graph, we can draw a picture as described and shown above, but place arrows on every edge corresponding to its direction.

In general, a **weight** on a graph G is some function $c:E(G)\to\mathbb{R}$.

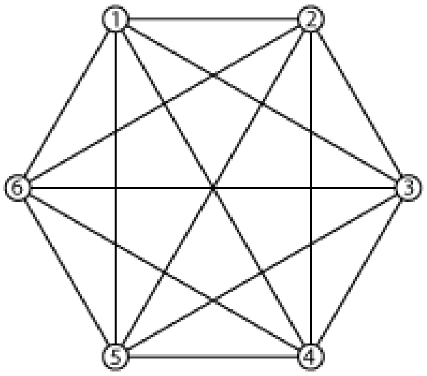
A **flow** (G,c) is a directed graph $G=(V,E,f)$ paired with a weight function such that the weight "going into" any vertex is the same amount as the weight "going out" of that vertex. To make this more formal, define sets

- $f^+(v)=\{e\in E(G)|f(e)=(v,x),x\in V(G)\},\ \forall v\in V(G)$
- $f^-(v)=\{e\in E(G)|f(e)=(x,v),x\in V(G)\},\ \forall v\in V(G)$

Then, formally stated, our requirement on the weight function is $\sum_{e\in f^+(v)} c(e)=\sum_{e\in f^-(v)} c(e),\ \forall v\in V(G).$

Special Graphs

Some graphs occur frequently enough in graph theory that they deserve special mention. One such graphs is the *complete graph* on n vertices, often denoted by K_n. This graph consists of n vertices, with each vertex connected to every other vertex, and every pair of vertices joined by exactly one edge. Another such graph is the *cycle graph* on *n* vertices, for *n* at least 3. This graph is denoted C_n and defined by V := {1,2,..,n} and E := . Even easier is the *null graph* on *n* vertices, denoted N_n; it has *n* vertices and no edges! Note that $N_1 = K_1$ and $C_3 = K_3$.



The complete graph on 6 vertices

Some Terms

Two vertices are said to be *adjacent* if there is an edge joining them. The word *incident* has two meanings:

- An edge *e* is said to be incident to a vertex *v* if *v* is an endpoint of *e*.
- Two edges are also incident to each other if both are incident to the same vertex.

Two graphs *G* and *H* are said to be *isomorphic* if there is a one-to-one function from (or, if you prefer, one-to-one correspondence between) the vertex set of *G* to the vertex set of *H* such that two vertices in *G* are adjacent if and only if their images in *H* are adjacent. (Technically, the multiplicity of the edges must also be preserved, but our definition suffices for simple graphs.)

Subgraphs

A *subgraph* is a concept akin to the subset. A subgraph has a subset of the vertex set V, a subset of the edge set E, and each edge's endpoints in the larger graph has the same edges in the subgraph. A

A subgraph H of G is *generated* by the vertices { $a, b, c, \dots$ } $\in H$ if the edge set of H consists of all edges in the edge set of G that joins the vertices in $H = \{ a, b, c, \dots \}$.
A *path* is a sequence of edges $< e_1, \dots, e_N >$ such that e_i is adjacent to e_{i+1} for all i from 1 to N-1. Two vertices are said to be connected if there is a path connecting them.

Trees and Bipartite Graphs

A *tree* is a graph that is (i) connected, and (ii) has no cycles. Equivalently, a tree is a connected graph with exactly $n - 1$ edges, where there are n nodes in the tree.

A *Bipartite graph* is a graph whose nodes can be partitioned into two disjoint sets U and W such that every edge in the graph is incident to one node in U and one node in W. A tree is a bipartite graph.

A *complete bipartite graph* is a bipartite graph in which each node in U is connected to every node in W; a complete bipartite graph in which U has n vertices and V has m vertices is denoted $K_{n,m}$.

Adjacent,Incident,End Vertices

Self loops,Parallel edges,Degree of Vertex

Pendant Vertex : Vertex Degree one "Pendant Vertex" Isolated Vertex : Vertex Degree zero "Isolated Vertex"

Hamiltonian and Eulerian Paths

Hamiltonian Cycles: A Hamiltonian Cycle received its name from Sir William Hamilton who first studied the travelling salesman problem. A Hamiltonian cycle is a path that visits every vertex once and only once i.e. it is a walk, in which no edge is repeated (a trail) and therefore a trail in which no vertex is repeated (a path). Note also it is a cycle, the last vertex is joined to the first.

A graph is said to be Eulerian if it is possible to traverse each edge once and only once, i.e. it has no odd vertices or it has an even number of odd vertices (semi-Eulerian). This has implications for the Königsberg problem. It may be easier to imagine this as if it is possible to trace the edges of a graph with a pencil without lifting the pencil off the paper or going over any lines.

Planar Graphs

A *planar graph* is an undirected graph that can be drawn on the plane or on a sphere in such a way that no two edges cross, where an edge $e = (u, v)$ is drawn as a continuous curve (it need not be a straight line) from u to v.

Kuratowski proved a remarkable fact about planar graphs: A graph is planar if and only if it does not contain a subgraph homeomorphic to K_5 or to $K_{3,3}$. (Two graphs are said to be homeomorphic if we can shrink some components of each into single nodes and end up with identical graphs. Informally, this means that non-planar-ness is caused by only two things -- namely, having the structure of K_5 or $K_{3,3}$ within the graph).

Coloring Graphs

A graph is said to be planner if it can be drawn on a plane in such way that no edges cross one anather except of course of vertices

Each term, the Schedules Office in some university must assign a time slot for each final exam. This is not easy, because some students are taking several classes with finals, and a student can take only one test during a particular time slot. The Schedules Office wants to avoid all conflicts, but to make the exam period as short as possible.

We can recast this scheduling problem as a question about coloring the vertices of a graph. Create a vertex for each course with a final exam. Put an edge between two vertices if some student is taking both courses. For example, the scheduling graph might look like this: Next, identify each time slot with a color. For example, Monday morning is red, Monday afternoon is blue, Tuesday morning is green, etc.

Assigning an exam to a time slot is now equivalent to coloring the corresponding vertex. The main constraint is that adjacent vertices must get different colors; otherwise, some student has two exams at the same time. Furthermore, in order to keep the exam period short, we should try to color all the vertices using as few different colors as possible. For our example graph, three colors suffice: red, green, blue.

The coloring corresponds to giving one final on Monday morning (red), two Monday afternoon (blue), and two Tuesday morning (green)...

K Coloring

Many other resource allocation problems boil down to coloring some graph. In general, a graph G is kcolorable if each vertex can be assigned one of k colors so that adjacent vertices get different colors. The smallest sufficient number of colors is called the chromatic number of G. The chromatic number of a graph is generally difficult to compute, but the following theorem provides an upper bound:

Theorem 1. A graph with maximum degree at most k is (k + 1)colorable.

Proof. We use induction on the number of vertices in the graph, which we denote by n. Let P(n) be the proposition that an nvertex graph with maximum degree at most k is (k + 1)colorable. A 1 vertex graph has maximum degree 0 and is 1colorable, so P(1) is true.

Now assume that P(n) is true, and let G be an (n + 1)vertex graph with maximum degree at most k. Remove a vertex v, leaving an nvertex graph G . The maximum degree of G is at most k, and so G is (k + 1)colorable by our assumption P(n). Now add back vertex v. We can assign v a color different from all adjacent vertices, since v has degree at most k and k + 1 colors are available. Therefore, G is (k + 1)colorable. The theorem follows by induction.

Weighted Graphs

A **weighted graph** associates a label (weight) with every edge in the graph. Weights are usually real numbers, and often represent a "cost" associated with the edge, either in terms of the entity that is being modeled, or an optimization problem that is being solved.

Discrete Mathematics/Recursion

In this section we will look at certain mathematical processes which deal with the fundamental property of ***recursion*** at its core.

What is recursion?

Recursion, simply put, is the process of describing an action in terms of itself. This may seem a bit strange to understand, but once it "clicks" it can be an extremely powerful way of expressing certain ideas.

Let's look at some examples to make things clearer.

Exponents

When we calculate an exponent, say x^3, we multiply x by itself three times. If we have x^5, we multiply x by itself five times.

However, if we want a recursive definition of exponents, we need to define the action of taking exponents in terms of itself. So we note that x^4 for example, is the same as $x^3 \times x$. But what is x^3? x^3 is the same as $x^2 \times x$. We can continue in this fashion up to $x^0=1$. What can we say in general then? Recursively,

$$x^{\mathrm{n}} = x \times (x^{\mathrm{n-1}})$$

with the fact that

$$x^0=1$$

We need the second fact because the definitions fail to make sense if we continue with negative exponents, and we would continue indefinitely!

Recursive definitions

In general, to create a recursive definition of some concept, we need to do **two** things and two things only:

- create a definition in terms of itself, changing it somehow (for example, we change x^{n} to be $x \times x^{\boldsymbol{n\text{-}1}}$)
- create a non-recursive definition as a "base" (in the above example, our "base" is $x^0=1$)

These two cases are known as the *stepping case* (or *recursive case*), and the *stopping case* (or *base case*).

Recurrence relations

In mathematics, we can create recursive *functions*, which depend on its previous values to create new ones. We often call these *recurrence relations*.

For example, we can have the function :$f(x)=2f(x\text{-}1)$, with $f(1)=1$ If we calculate some of f's values, we get

1, 2, 4, 8, 16, ...

However, this sequence of numbers *should* look familiar to you! These values are the same as the function 2^x, with x = 0, 1, and so on.

What we have done is found a *non-recursive* function with the same values as the *recursive* function. We call this *solving* the recurrence relation.

Linear recurrence relations

We will look especially at a certain kind of recurrence relation, known as *linear*.

Here is an example of a linear recurrence relation:

$f(x)=3f(x-1)+12f(x-2)$, with f(0)=1 and f(1)=1

Instead of writing $f(x)$, we often use the notation a_{n} to represent $a(n)$, but these notations are completely interchangeable.

Note that a linear recurrence relation should always have stopping cases, otherwise we would not be able to calculate $f(2)$, for example, since what would $f(1)$ be if we did not define it? These stopping cases when we talk about linear recurrence relations are known as *initial conditions*.

In general, a linear recurrence relation is in the form

$a_{\mathrm{n}}=A_1a_{n\text{-}1} + A_2a_{n\text{-}2} + ... + A_ja_{n\text{-}\mathrm{j}}$
with $f(t_1)=u_1, f(t_2)=u_2, ..., f(t_j)=u_{\mathrm{j}}$ as initial conditions.

The number j is important, and it is known as the *order* of the linear recurrence relation. Note we always need at least j initial conditions for the recurrence relation to make sense.

Recall in the previous section we saw that we can find a nonrecursive function (a *solution*) that will take on the same values as the recurrence relation itself. Let's see how we can solve some linear recurrence relations - we can do so in a very systematic way, but we need to establish a few theorems first.

Solving linear recurrence relations

Sum of solutions

This theorem says that:

If $f(n)$ and $g(n)$ are both solutions to a linear recurrence relation $a_n=Aa_{n\text{-}1}+Ba_{n\text{-}2}$, their sum is a solution also.

This is true, since if we rearrange the recurrence to have $a_n\text{-}Aa_{n\text{-}1}\text{-}Ba_{n\text{-}2}=0$ And we know that $f(n)$ and $g(n)$ are solutions, so we have, on substituting into the recurrence

$f(n)\text{-}Af(n\text{-}1)\text{-}Bf(\mathrm{n}\text{-}2)=0$

$g(n)\text{-}Ag(n\text{-}1)\text{-}Bg(\mathrm{n}\text{-}2)=0$

If we substitute the sum $f(n)+g(n)$ into the recurrence, we obtain

$(f(n)+g(n))\text{-}A(f(n\text{-}1)+g(n\text{-}1))\text{-}B((f(n\text{-}2)+g(n\text{-}2))=0$

On expanding out, we have

$f(n)\text{-}Af(n\text{-}1)\text{-}Bf(\mathrm{n}\text{-}2)+g(n)\text{-}Ag(n\text{-}1)\text{-}Bg(\mathrm{n}\text{-}2)$

But using the two facts we established first, this is the same as

0+0=0

So $f(n)+g(n)$ is indeed a solution to the recurrence.

General solution

The next theorem states that:

Say we have a second-order linear recurrence relation, a_n-Aa_{n-1}-Ba_{n-2}=0, with supplied initial conditions.

Then αr^n is a solution to the recurrence, where r is a solution of the quadratic equation

x^2-Ax-B=0

which we call the *characteristic equation*.

We guess (it doesn't matter why, accept it for now) that αr^n may be a solution. We can prove that this is a solution IF (and only if) it solves the characteristic equation ;

We substitute αr^n (r not zero) into the recurrence to get

αr^n-$A\alpha r^{n-1}$-$B\alpha r^{n-2}$=0

then factor out by αr^{n-2}, the term farthest on the right

$\alpha r^{n-2}(r^2-Ar-B)=0$

and we know that r isn't zero, so r^{n-2} can never be zero. So r^2-Ar-B must be zero, and so αr^n, with r a solution of r^2-Ar-B=0, will indeed be a solution of the linear recurrence. Please note that we can easily generalize this fact to higher order linear recurrence relations.

Where did this come from? Why does it work (beyond a rote proof)? Here's a more intuitive (but less mathematically rigorous) explanation.

Solving the *characteristic equation* finds a function that satisfies the linear recurrence relation, and conveniently doesn't require the summation of all n terms to find the *n*th one.

We want : a function F(n) such that F(n) = A * F(n-1) + B * F(n-2)

We solve : x^2 = A* x + B, and call the solution(s) *r*. There can be more than one value of r, like in the example below!

We get : a function F(n) = r^n that satisfies F(n) = A * F(n-1) + B * F(n-2)

Let's check: Does r^n = A*r^{n-1} + B*r^{n-2} ? Divide both sides by r^{n-2} and you get r^2 = A*r + B, which must be true because r is a solution to x^2 = A* x + B

Why does *ar^n also satisfy the recurrence relation?** If F(n)is a solution to the recurrence relation, so is F(n)+ F(n), based on the "Sum of Solutions" theorem above. One can then take that sum, 2*F(n), and add another F(n) to get 3*F(n), and it will still satisfy the recurrence (and so on...). Thus any whole number multiple of F(n), such as *a**F(n) will satisfy the recurrence relation (*a* can also be any fraction and probably any real number at all, but I'm too lazy to adapt the current explanation). Because r^n satisfies the recurrence, so does *a**r^n.

Because we have a second order recurrence, the general solution is the sum of two solutions, corresponding to the two roots of the characteristic equation. Say these are r and s. The the general solution is C(r^n)+D(s^n) where C,D are some constants. We find them using the two (there must be two so that we can find C and D) starting values of the relation. Substituting these into the general solution will give two equtions which we can (hopefully) solve.

Example

Let's work through an example to see how we can use the above theorems to solve linear recurrence relations. Examine the function $a(n)$ given here

$a(n)=a(n-1)+2a(n-2)$

The characteristic equation of this recurrence relation is

r^2-r-2 = 0 from above, as A=1 and B=2

i.e. (r-2)(r+1)=0 which has roots 2, -1.

So the general solution is C(2^n)+D$(-1)^n$.

To find C and D for this specific case, we need two starting values, let's say *a*(*1*) = 0 and *a*(2) = 2. These give a system of two equations
0 = C(2^1)+D(-1)^1
2 = C(2^2)+D(-1)^2
Solving these two equations yields: C = 1/3 , D = 2/3, so the solution is 1/3*(2^n)+2/3*(-1)^n.

Discrete Mathematics/Axiomatic set theory

See also: Topology/Set Theory

Discrete Mathematics/Zermelo-Frankel Axioms

Zermelo–Fraenkel set theory, with the axiom of choice, commonly abbreviated ZFC, is the standard form of axiomatic set theory and as such is the most common foundation of mathematics.

ZFC consists of a single primitive notion, that of set, and a single assumption, namely that all mathematical objects are sets. There is a single primitive binary relation, set membership; that set a is a member of set b is written $a \in b$ (usually read "a is an element of b" or "a is in b"). The axioms of ZFC govern how sets behave and interact.

The axioms

1. Axiom of extensionality: Two sets are equal (are the same set) if they have the same elements.

$$\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y].$$

The converse of this axiom follows from the substitution property of equality. If the background logic does not include equality "=", *x*=*y* may be defined as abbreviating ∀*z*[*z*∈*x*↔*z*∈*y*] ∧ ∀*z*[*x*∈*z*↔*y*∈*z*], in which case this axiom can be reformulated as $\forall x \forall y [\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow \forall z (x \in z \Leftrightarrow y \in z)]$ — if *x* and *y* have the same elements, then they belong to the same sets.

2. Axiom of regularity (also called the *Axiom of foundation*): Every non-empty set *x* contains a member *y* such that *x* and *y* are disjoint sets.

$$\forall x [\exists y (y \in x) \Rightarrow \exists y (y \in x \land \neg \exists z (z \in y \land z \in x))].$$

3. Axiom schema of specification (also called the axiom schema of *separation* or of *restricted comprehension*): If *z* is a set, and ϕ is any property which may characterize the elements *x* of *z*, then there is a subset *y* of *z* containing those *x* in *z* which satisfy the property. More formally:

$$\forall z \forall w_1 \ldots w_n \exists y \forall x [x \in y \Leftrightarrow (x \in z \land \phi)].$$

The axiom of specification can be used to prove the existence of the empty set, denoted $\varnothing$, once the existence of at least one set is established (see above). A common way to do this is to use an instance of specification for a property which all sets do not have. For example, if *w* is a set which already exists, the empty set can be constructed as

$$\varnothing = \{u \in w \mid (u \in u) \land \neg (u \in u)\} .$$

If the background logic includes equality, it is also possible to define the empty set as

$$\varnothing = \{u \in w \mid \neg (u = u)\} .$$

Thus the axiom of the empty set is implied by the nine axioms presented here. The axiom of extensionality implies the empty set is unique, if it exists. It is common to make a definitional extension that adds the symbol $\varnothing$ to the language of ZFC.

4. Axiom of pairing: If *x* and *y* are sets, then there exists a set which contains *x* and *y* as elements.

$$\forall x \forall y \exists z (x \in z \wedge y \in z).$$

5. Axiom of union: For any set $\mathcal{F}$ there is a set *A* containing every set that is a member of some member of $\mathcal{F}$.

$$\forall \mathcal{F} \, \exists A \, \forall Y \, \forall x (x \in Y \wedge Y \in \mathcal{F} \Rightarrow x \in A).$$

6. Axiom schema of collection: This axiom states that if the domain of a function *f* is a set, and *f*(*x*) is a set for any *x* in that domain, then the range of *f* is a subclass of a set, subject to a restriction needed to avoid paradoxes.

7. Axiom of infinity: Let $S(x)$ abbreviate $x \cup \{x\}$, where x is some set. Then there exists a set *X* such that the empty set $\varnothing$ is a member of *X* and, whenever a set *y* is a member of *X*, then $S(y)$ is also a member of *X*.

$$\exists X \left[\varnothing \in X \wedge \forall y (y \in X \Rightarrow S(y) \in X)\right].$$

More colloquially, there exists a set *X* having infinitely many members.

8. Axiom of power set: Let $z \subseteq x$ abbreviate $\forall q (q \in z \Rightarrow q \in x).$ For any set *x*, there is a set *y* which is a superset of the power set of *x*. The power set of *x* is the class whose members are every possible subset of *x*.

$$\forall x \exists y \forall z [z \subseteq x \Rightarrow z \in y].$$

Alternative forms of axioms **1–8** are often encountered. Some ZF axiomatizations include an axiom asserting that the empty set exists. The axioms of pairing, union, replacement, and power set are often stated so that the members of the set *x* whose existence is being asserted, are just those sets which the axiom asserts *x* must contain.

9. Well-ordering theorem: For any set *X*, there is a binary relation *R* which well-orders *X*. This means *R* is a linear order on *X* such that every nonempty subset of *X* has a member which is minimal under *R*.

$$\forall X \exists R (R \text{ well-orders } X).$$

Given axioms **1-8**, there are many statements provably equivalent to axiom **9**, the best known of which is the axiom of choice (AC), which goes as follows. Let *X* be a set whose members are all non-empty. Then there exists a function *f*, called a "choice function," whose domain is *X*, and whose range is a set, called the "choice set," each member of which is a single member of each member of *X*. Since the existence of a choice function when *X* is a finite set is easily proved from axioms **1-8**, AC only matters for certain infinite sets. AC is characterized as nonconstructive because it asserts the existence of a choice set but says nothing about how the choice set is to be "constructed." Much research has sought to characterize the definability (or lack thereof) of certain sets whose existence AC asserts.

Discrete Mathematics/Number representations

You are already familiar with writing a number down, and having it mean a certain combination of tens, hundreds, and so on. This is one form of **number representation**, but there are others. We will look at number bases and continued fractions.

Number bases

You are already familiar with base-10 number representation. For example, the number 2818 is the same as

$$2\times10^3+8\times10^2+1\times10^1+8\times10^0$$

We can replace the number 10 here with any number and we obtain a different number. In general, we can represent an integer *n* in a base *b* by the following:

$$a_k b^k+a_{k-1} b^{k-1}+...+a_0 b^0$$

where the a_i are all less than *b*.

We write a number base *b* as $(a_k a_{k-1}...a_0)_b$.

For example, if we have the numeral 243 in base 6, we write it $(243)_6$. When we are in base 10 we simply write the number: for example the numeral 155 in base 10 is simply written 155.

However, given a number in a base *b*, how can we convert it to our natural base 10 system? Likewise, how can we convert a number from our base 10 system to base *b*?

The first is relatively easy, the other more difficult.

Converting base *b* to base 10

We simply use the definition of a base-*b* number to convert a base-*b* number to base 10 - that is we simply multiply out.

For example

$$(919)_{12}=9\times12^2+12^1+9=1317.$$

Converting base 10 to base *b*

This task however is slightly more difficult, and there are several ways of performing this task.

One method is to write each step using the division algorithm from the ../Number theory/ section. For example, if we wish to convert 1317 to base 12:

$$1317 = 12 \times 109 + 9$$

$$109 = 12 \times 9 + 1$$

$$9 = 12 \times 0 + 9$$

So in base 12, $(919)_{12}$=1317.

Real numbers

We've just seen how we can convert *integers* from base to base, but how do we work with converting *real* numbers?

Recall in base 10 we write a number such as 11.341 as

$$1\times10^{1}+1\times10^{0}+3\times10^{-1}+4\times10^{-2}+1\times10^{-3}$$

and so we can extend our definition above of a base-*b* number to be

$a_k b^k + a_{k-1} b^{k-1} + ... + a_0 b^0 + a_{-1} b^{-1} + ...$

where the a_i are all less than *b*, and the sum could terminate or go on indefinitely.

Again, how are we to convert these numbers from base to base? We can convert the integral part, but what about the *fractional part* (the part less than 1)?

Converting fractional *n* to base-*b*

Say we wish to convert .341 in base 10 to base 6.

We write a table, using the following rules

$$c_i = \lfloor 6\gamma_{i-1} \rfloor$$
$$\gamma_i = 6\gamma_{i-1} - c_i$$

i	c_i	γ_i	$6\gamma_i$
0	0	.341	2.046
1	2	.046	0.276
2	0	.276	1.656
3	1	.656	3.936
4	3	.936	5.616
5	5	.616	3.696
6	3	.696	4.176
7	4	.176	1.056
8	1	.056	0.336
9	0	.336	2.016

It looks like this expansion will go on forever! We need to calculate for further values of i to see whether we hit a repeat value of γ_i to see whether we get a repetition.

So we have the approximation that .341 is near to $(.20135341)_6$. (*Calculate this using the definition. How close is our approximation?*)

If we obtain a base-*b* representation for example, that looks something like $(.18191819181918191819...)_b$ we call the representation *periodic*. We often write this as

$$(.\overline{1819})_b$$

We use this same procedure to convert a fractional number to base-*b* by replacing the 6 above with *b*.

Converting fractional *n* to base 10

We have a nifty trick we can use to convert a fractional *n* in base-*b* to base 10 provided the representation repeats. Let us look at an example:

Consider $(.\overline{3145})_7 = \alpha$. Now then

$$(3145.\overline{3145})_7 = 7^4\alpha$$

And now

$$(3145)_7 + (.\overline{3145})_7 = 7^4\alpha$$

which is

$$(3145)_7 + \alpha = 7^4\alpha$$

Then

$$(3145)_7 = 7^4\alpha - \alpha$$
$$(3145)_7 = (7^4 - 1)\alpha$$

And finally

$$\frac{(3145)_7}{7^4 - 1} = \alpha$$

On converting $(3145)_7$ to base 10, we obtain the following

$$\alpha = 1111/2400$$

Continued fractions

In a sense, the base-*b* representation is nice, but it has a few shortcomings in respect to accuracy. We cannot reliably represent the number $\sqrt{2}$ using base-*b* representation. This is where the *continued fraction* representation comes in handy, which has some nice properties regarding quadratic irrationals.

A *continued fraction* is a number in the form

$$q_0 + \cfrac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots}}}$$

Since this notation is clearly rather cumbersome, we abbreviate the above to

$$[q_0; q_1, q_2, q_3, \dots]$$

Again we ask ourselves how can we convert from and to this number representation? Again converting from is simpler than converting to.

Converting from continued fraction representation

We simply use our definition of the continued fraction to convert from a continued fraction. This may look difficult, but in fact is quite simple depending on which end one starts with. Let's look at an example

Consider

$$\alpha = [3; 1, 2, 5]$$

Now, we work from right to left. We first have the fraction

$$\frac{1}{5}$$

The next digit 2 tells us to perform

$$2 + \frac{1}{5} = 11/5$$

and then take the reciprocal to get

$$\frac{5}{11}$$

Now the next digit 1 tells us to perform

$$1+\frac{5}{11}=\frac{16}{11}$$

and then to take the reciprocal to get

$$\frac{11}{16}$$

Now we must add q_0 which is always greater than 1 and we get the result:

$$\alpha=\frac{59}{16}$$

Converting to continued fraction representation

Again, we draw up a table.

Consider the fraction 12/22, and use the following rules in the table

$\theta_i=\theta_{i-1}-q_{i-1}$

$$q_i=\lfloor\theta_i^{-1}\rfloor$$

i	θ_i	θ_i^{-1}	q_i
0	12/22	.	0
1	12/22	22/12	1
2	5/6	6/5	1
3	1/5	5/1	5

(stop since next row will be full of 0s)

So now the continued fraction for 12/22 is [0; 1, 1, 5].

Converting a periodic continued fraction to quadratic irrational

Firstly, we make note of a nice property of periodic continued fractions (where the sequence of q_i repeat), that

> every periodic continued fraction is a number in the form
>
> $$\frac{a\pm\sqrt{b}}{c}\text{ for }a,b,c\in\mathbb{Z}$$

For example, consider the continued fraction

$$\begin{aligned}\alpha &= [2;2,1,2,2,1...]\\ &= [2;\overline{2,1,2}]\end{aligned}$$

Now

$$[2;\overline{2,1,2}]=[2;2,1,\overline{2,2,1}]$$

which we can rewrite as

$$\alpha=2+\frac{1}{2+\frac{1}{1+\frac{1}{\alpha}}}$$

Now we can simplify to obtain

$$\alpha=2+\frac{1}{2+\frac{1}{\frac{\alpha+1}{\alpha}}}$$

$$\alpha = 2 + \frac{1}{2 + \frac{\alpha}{\alpha+1}}$$

$$\alpha = 2 + \frac{1}{\frac{3\alpha+2}{\alpha+1}}$$

$$\alpha = 2 + \frac{\alpha+1}{3\alpha+2}$$

$$\alpha = \frac{7\alpha+5}{3\alpha+2}$$

$$\alpha(3\alpha+2) = 7\alpha+5$$

$$\alpha(3\alpha+2) - 5 = 7\alpha$$

$$3\alpha^2 + 2\alpha - 5 = 7\alpha$$

$$3\alpha^2 + 2\alpha - 7\alpha - 5 = 0$$

$$3\alpha^2 - 5\alpha - 5 = 0$$

which is a quadratic equation and can be solved to obtain

$$\alpha = \frac{5+\sqrt{85}}{6}.$$

Note that we can always roll up the continued fraction into the form (aα+b)/(cα+d)=α, which demonstrates the point that every quadratic irrational has a repeating continued fraction representation

Convergents

Say we have a continued fraction [q_0; q_1, ...] which represents a number *n*. Let us examine the following series of fractions [q_0], [q_0; q_1], [q_0; q_1, q_2] and so on. Each element of the series is known as a *convergent*. It turns out that the series of convergents provide the best rational approximations to *n*.

These can be calculated from the continued fraction representation, but also from the calculation table. Let us take $\sqrt{6}$.

Continue as before, but place an extra -1 row, and set u_{-1}=1, v_{-1}=0. Iterate with the rules

$$u_{i+1} = q_{i+1}u_i + v_{i-1}$$

$$v_{i+1} = q_{i+1}v_i + v_{i-1}$$

i	θ_i	θ_i^{-1}	q_i	u_i	v_i
-1				1	0
0	$\sqrt{6}$		2	2	1
1	$2-\sqrt{6}$	$1+\sqrt{3/2}$	2	5	2
2	$-1+\sqrt{3/2}$	$2+\sqrt{6}$	4	22	9
3	$-2+\sqrt{6}$	$1+\sqrt{3/2}$	2	49	20

and the sequence repeats and the continued fraction is [2; 2, 4, 2, 4, ...]. We can continue the process to generate more convergents - the convergents are 2, 5/2, 22/9, 49/20, ...

Discrete Mathematics/Modular arithmetic

We have already considered moduli and modular arithmetic back in ../Number theory/, however in this section we will take a more in depth view of modular arithmetic.

For revision, you should review the material in number theory if you choose.

Simultaneous equations

When we speak of simultaneous equations with relation to modular arithmetic, we are talking about simultaneous solutions to sets of equations in the form

$x \equiv a_1 \text{ (mod m}_1\text{)}$

:

:

$x \equiv a_k \text{ (mod m}_k\text{)}$

There are two principal methods we will consider, *successive substitution* and the *Chinese remainder theorem*.

Successive substitution

The method of successive substitution is that where we use the definition of the modulus to rewrite these simultaneous equations, and then successively make substitutions.

It will probably be best to motivate the idea with an example.

Example: Solve $3x \equiv 10 \text{ (mod 19)}$, and $x \equiv 19 \text{ (mod 21)}$ using successive substitution.

First:

$3x \equiv 10 \text{ (mod 19)}$

Find the inverse of 3 in $\mathbf{Z}_{19}$; 3^{-1}=-6, then

$x \equiv -60 \text{ (mod 19)}$

$x \equiv 16 \text{ (mod 19)}$

$x = 16 + 19j \ \exists \ j \in \mathbf{Z}$ (*)

Substitute in the second equation

$(16+19j) \equiv 19 \text{ (mod 21)}$

$19j \equiv 3 \text{ (mod 21)}$

Find the inverse of 19 in $\mathbf{Z}_{21}$; 19^{-1}=10

$j = 30 \text{ (mod 21)}$

$j = 9 \text{ (mod 21)}$

Writing in the equivalent form

$j = 9 + 21k \ \exists \ k \in \mathbf{Z}$

Substituting back j in (*)

$x = 16 + 19(9+21k)$

$x = 187+399k$

Writing back in the first form

$x \equiv 187 \text{ (mod 399)}$

which is our solution.

Chinese remainder theorem

The *Chinese remainder theorem* is a method for solving simultaneous linear congruences **when the moduli are coprime**.

Given the equations

> $x \equiv a_1 \pmod{m_1}$
>
> :
>
> :
>
> $x \equiv a_k \pmod{m_k}$

multiply the moduli together, i.e. $N=m_1m_2...m_k$, then write $n_1=N/m_1$, ..., $n_k=N/m_k$.
We then set y_i be the inverse of n_i mod m_i for all i, so $y_in_i=1$ mod m_i.
Our solution will be

> $x \equiv a_1y_1n_1+...+a_ky_kn_k \pmod{N}$

To see why this works consider what values x mod m_k takes. The term $a_ky_kn_k$ mod m_k becomes equal to a_k as $y_kn_k=1$ mod m_k, and all the terms $a_jy_jn_j$ mod m_k become equal to zero as when $j \neq k$ m_k is a factor of n_j.
The Chinese Remainder Theorem is of immense practical use, as if we wish to solve an equation mod M for some large M, we can instead solve it mod p for every prime factor of M and use CRT to obtain a solution mod M.

Powers and roots

This section deals with looking powers of numbers modulo some modulus. We look at efficient ways of calculating

> $a^b \pmod{m}$

If we tried to calculate this normally - by calculating a^b and then taking the modulus - it would take an *exorbitant* amount of time. However some of the theory behind modular arithmetic allows us a few shortcuts.

We will look at some of these and the theory involved with them.

Fermat's (little) Theorem

Fermat's theorem allows us to see where $a^b \pmod{m}$ is 1. This has an application in disproving primality.

It states

> If p is prime, and gcd(a,p)=1, then, in $\mathbf{Z}_p$
> $a^{p-1}=1$.

So, for example, $13^{10}=1$ in $\mathbf{Z}_{11}$.

Primitive elements

If in $\mathbf{Z}_n$, can we write some elements as powers of an element? This is conceivably possible.

Let's look at $\mathbf{Z}_3$.

> $2^0=1$
>
> $2^1=2$
>
> $2^2=1$

The elements {1,2} constitute in fact :$\mathbf{Z}_3^*$.

Generally, we have

> If p prime, then there is an element $g \in \mathbf{Z}_p^*$ such that every element of $\mathbf{Z}_p^*$ is a power of g.

Orders

We can express this idea in a different way, using the concept of the *order*. We denote the order of $a \in \mathbf{Z}_n^*$ by the smallest integer k written $O_n(a)$ such that

$a^k=1$ in $\mathbf{Z}_n$.

For example, $O_n(-1)=2$ for all n except 2, since

$(-1)^2=1$

except when n = 2, since in that field -1 = 1 and thus has order 1.

Note if $\gcd(a,n)\neq 1$, that is, $a \notin \mathbf{Z}_n^*$, the order *is not defined*.

Properties of orders

The orders obey some properties, the first of which was originally proven by Lagrange:

If p prime, gcd(a,p)=1,

- $O_p(a)$ divides p-1
- a is primitive iff $O_p(a)=p-1$

Orders and finding primitive elements

Given these facts above, we can find primitive elements in $\mathbf{Z}_p$ for $p > 2$ fairly easily.

Using the above facts, we only need to check $a^{(p-1)/p}i=x_i$ in $\mathbf{Z}_p$ for all i, where the p_i are the prime factors of p-1. If any of the x_i are 1, a is not a primitive element, if none are, it is.

Example: Find a primitive element of $\mathbf{Z}_{11}$.

Try 2. p-1 = 10 = 2 . 5 Check:

$2^{10/2}=2^5=10$

$2^{10/5}=2^2=4$

Neither is 1, so we can say that 2 is a primitive element in $\mathbf{Z}_{11}$.

Problem set

Given the above, answer the following. (Answers follow to even-numbered questions)

1. Is 4 primitive in $\mathbf{Z}_{13}$?
2. Is 5 primitive in $\mathbf{Z}_{23}$?
3. Find a primitive element of $\mathbf{Z}_5$.
4. Find a primitive element of $\mathbf{Z}_{19}$.

Answers

2. Yes: In $\mathbf{Z}_{23}$, (23-1)=2*11, and $5^{22/11}=2$, $5^{22/2}=22$ and then $5^{22}=1$. No lesser base gives this.

4. 2. Check: (19-1) has distinct prime factors 2 and 3. In $\mathbf{Z}_{19}$, $2^{18/2}\neq 1$ and $2^{18/3}\neq 1$ but $2^{18}=1$ so 2 is primitive.

Euler's totient function

Euler's totient function is a special function that allows us to generalize Fermat's little theorem above.

It is defined as

$\varphi(n) = |\mathbf{Z}_n^*|$

$=|\{a\in\mathbf{Z}|1 \leq a \leq n \text{ and } \gcd(a,n) = 1\}|$

that is the number of elements that have inverses in $\mathbf{Z}_n$

Some results

We have the following results leading on from previous definitions.

1. φ(p) = p - 1
2. φ(p^k) = p^k-p^{k-1}
3. φ(mn)=φ(m)φ(n) for gcd(m,n)=1
4. For any integer n, the sum of the totient values of each of its divisors equals n.

In other symbols: $\sum_{d \ divisor \ of \ n} \phi(d) = n$.

Proof of 2.: There are p^k elements in $\mathbf{Z}_p$k. The non-invertible elements in $\mathbf{Z}_p$k are the multiples of p and there are p^{k-1} of them: p, 2p, 3p, ..., (p^{k-1}-1)p, p^k. Removing the non-invertible elements from the invertible ones leaves p^k-p^{k-1} left. ▯

Corollary to 1, 2 and 3: If n has distinct prime factors (i.e. not counting powers) p_i for i=1,...,r we have

$$\phi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

For example:

16=2^4, so φ(16)=(16)(1-1/2)=16/2=8

φ(11)=(11)(1-1/11)=(11)(10/11)=10

(confirm from before 11 prime so φ(11)=11-1=10).

Proof of 3.: We can prove this equality using a special case of the Chinese Remainder Theorem, where the CRT is now just a system of 2 congruences, namely:

x == a_1 (mod m)

x == a_2 (mod n)

(remember that the CRT is applicable here because m and n are assumed coprime in the equality).

Note that a_1 can take on m values (from 0 to m-1), and a_2 can take on n values (from 0 to n-1). Also note that, for each and everyone of the m*n (a_1, a_2) tuples, there is a unique solution x that is strictly smaller than m*n. Moreover, for each x strictly smaller than m*n, there is a unique tuple (a_1, a_2) verifying the congruence system (these two assertions are a component of the Chinese Remainder Theorem: a solution to the congruence system is unique modulo m*n).

With this bijective uniqueness property in mind, the proof is simple. Go through each x, from 0 to m*n-1, and show that if x is a totient of m*n (i.e., gcd (x,m*n) = 1), then a_1 is a totient of m and a_2 is a totient of n. Furthermore, you must also show that if a_1 and a_2 are totients of m and n respectively, then it follows that x must be a totient of m*n.

If gcd (x,m*n) = 1, then according to Bezout's identity, there exist X and Y integers such that x*X + m*n*Y = 1. Furthermore, we have:

x = a_1 + k*m

x = a_2 + q*n

Therefore, a_1*X + m*(k + n*Y) = 1,

should this be a_1*X + m*(k*X + n*Y) = 1 ??

so gcd (a_1,m) = 1, and therefore a_1 is a totient of m. Proceed similarly to prove that a_2 is a totient of n.

Proving the other direction is very similar in that it requires some simple replacement algebra.

So what have we shown? In the above we have shown that for every totient x of m*n, there is a unique tuple of totients of m on the one hand and n on the other hand. Furthermore, that for each tuple of totients of m on the one hand and n on the other hand, there is a unique totient of m*n. Therefore, phi(m*n) = phi(m)*phi(n).

Proof of 4.: Let Q(g) be the set of all integers between 1 and n inclusive, such that gcd(x,n) = g. Q(g) is nonempty if and only if g divides n. If g doesn't divide n, then good luck finding an x such that g is the greatest common DIVISOR of x and n. Secondly, if x belongs to Q(g) for a given g, then it can't belong to another Q(...), since, if n is fixed, then gcd(x,n) is unique, by definition of the GREATEST common divisor. Thirdly, for all x between 1 and n inclusive, there exists a g such that gcd (x,n) = g (in the "worst" case, it's 1). Put together, these three properties imply that the union of all the Q(g) sets (for each g a divisor of n), which are pairwise mutually exclusive, is the set {1,2,3,...,n}. And therefore, the sum of the cardinalities of each Q(g) equals n.

Now we show that |Q(g)| = φ(n/g).

One direction: Let x be an arbitrary member of Q(g) for some g. Therefore, we have that gcd (x,n) = g => gcd (x/g, n/g) = 1 => x/g belongs to the set of numbers coprime to n/g (whose cardinality of course is φ(n/g)). For diff\ erent x's, the two values x_1/g and x_2/g are distinct. So for each x in Q(g), there is a correspondingly unique x/g in the set of numbers coprime to n/g.

Other direction: Let x be an arbitrary member of the set of numbers coprime to n/g. This implies gcd (x,n/g) = 1 => gcd (xg,n) = g => xg belongs to Q(g). For different x's, the two values x_1g and x_2g are distinct. So for each x in the set of numbers coprime to n/g, there is a correspondingly unique xg in Q(g).

Therefore, |Q(g)| = φ(n/g).

Euler's theorem

We can now generalize Fermat's theorem to extend past just $\mathbf{Z}_n$.

Euler's theorem says:

> If $a \in \mathbf{Z}_n^*$, in $\mathbf{Z}_n^*$,
>
> > $a^{\varphi(n)}=1$
>
> equivalently if gcd(*a*,*n*)=1,
>
> > $a^{\varphi(n)} \equiv 1 \pmod{n}$

Example: Find 3^{216} in $\mathbf{Z}_{14}$. We need to calculate firstly φ(14)=φ(7)φ(2)=(7-1)(2-1)=6. Then write the exponent as: 216 = 6 × 36 So: $3^{216}=(3^6)^{36}$

But Euler's theorem tells us 3^6=1 in $\mathbf{Z}_{14}$ (i.e., mod 14) since $3^{\varphi(14)}$=1 in $\mathbf{Z}_{14}$ as above. So we have: $3^{216}=1^{36}=1$.

Calculating large powers efficiently

When Euler's or Fermat's theorem fails us in the calculation of a high power, there is a way to decompose an exponent down so calculation is still easy.

Let us work through an example as motivation.

Example. 5^{28} in $\mathbf{Z}_4$.

First write 28 in base 2 = $(11100)_2 = 2^4+2^3+2^2 = 16 + 8 + 4$

Now $5^{28} = 5^{16+8+4} = 5^{16}\, 5^8\, 5^4$ Now rewrite these powers of 2 as repeated exponents:

> $(((5^2)^2)^2)^2 \times ((5^2)^2)^2 \times (5^2)^2$

When you calculate each exponent, reduce mod 4 each time.

Problem set

Given the above, calculate the following powers. (Answers follow to even-numbered questions)

1. 3^{12} (mod 13)
2. 2^{42} (mod 43)
3. 6^{168} (mod 30)
4. 2^{252} (mod 19)
5. 2^{61} (mod 22)
6. 8^{13} (mod 5)
7. 11^{10} (mod 11) (*Tricky!*)

Answers

2. Since gcd(2,43)=1 and the exponent is one less than the modulus, use Fermat's theorem - the answer is 1

4. Observe that φ(19)=18 and 18|252. 252/18=14. Decompose the exponent then as $2^{18\times 14}$=$(2^{18})^{14}$=1.

6. Use fast exponentiation by squaring: the answer is 3

Discrete Mathematics/Polynomials

In this section we look at the **polynomial** in some commutative ring with identity. What is interesting is that studying polynomials over some commutative ring with identity acts very much like numbers; the same rules often are obeyed by both.

Definitions

A *polynomial* over some commutative ring with identity R is an expression in the form

$$\sum_{j=0}^{n} a_j x^j ; \forall a_j \in R, a_n \neq 0$$

and n ∈ **N**, and *x* is some indeterminate (*not* a variable).

Terminology

Given the first nonzero term in the polynomial, i.e. the term $a_n x^n$ above:

- a_n is called the *leading coefficient*
  - Given $7x^3+2x+5$, 7 is the leading coefficient
- the polynomial has *degree n*
  - $7x^3+2x+5$, 3 is the degree
- if a_n=1 the polynomial is termed *monic*
  - $7x^3+2x+5$ is *not monic*, whereas x^4 and x^5-3x+2 are *monic*.

In the above, if a_i=0 for all i, the polynomial is the *zero polynomial*.

Properties

Let R[x] be the set of all polynomials of all degrees. Clearly R is closed under addition and multiplication (although in a non-straightforward way), and thus we have that R[x] is itself a commutative ring with identity.

Assume now R is a field F; we do this so we can define some useful actions on polynomials

Division algorithm

Firstly recall the division algorithm for numbers, that each number can be decomposed into the form

n = qk+r

where q is the quotient and r the remainder and r<n.

Now, since we have that F is a field, we can do something similar with the polynomials over F, F[x].

If f(x), g(x) ∈ F[x], with g(x) nonzero:

f(x) = q(x)g(x)+r(x)

Again, q(x) is known as the quotient polynomial and r(x) the remainder polynomial. Furthermore, we have the degree of r(x) ≤ degree of f(x)

We perform divisions by polynomial long division. For brevity we omit the x^k terms. Here's an example. We divide x^3+x+2 by x-1. First write:

$$\begin{array}{cc|cccc} 1 & -1 & 1 & 0 & 1 & 2 \end{array}$$

Note we place a 0 in any polynomial not present. Now $x^3/x = x^2$, so we place a 1 in the second column to get

$$\begin{array}{cc|cccc} & & & 1 & & \\ 1 & -1 & 1 & 0 & 1 & 2 \end{array}$$

Multiply x^2 throughout the divisor x-1 to get x^3-x^2, which is (1 -1), so write this below like the following:

$$\begin{array}{cc|cccc} & & & 1 & & \\ 1 & -1 & 1 & 0 & 1 & 2 \\ & & 1 & -1 & & \end{array}$$

Now subtract (1 0) and (1 -1), drop the third 1 to get:

$$\begin{array}{cc|cccc} & & & 1 & & \\ 1 & -1 & 1 & 0 & 1 & 2 \\ & & 1 & -1 & & \\ & & & 1 & 1 & \end{array}$$

Now repeat, but divide by x^2 now (since we have subtracted and gotten (1 1) - x^2 + x), and continue in the same fashion, to get:

$$\begin{array}{cc|cccc} & & & 1 & 1 & 2 \\ 1 & -1 & 1 & 0 & 1 & 2 \\ & & 1 & -1 & & \\ & & & 1 & 1 & \\ & & & 1 & -1 & \\ & & & & 2 & 2 \\ & & & & 2 & -2 \\ & & & & & 4 \end{array}$$

So the quotient is x^2+x+2, and the remainder is 4.

Euclidean algorithm

Now we have a working division algorithm for polynomials, the Euclidean algorithm, and hence the gcd of two polynomials can readily be found.

Examples

Let's use a similar example above: what is gcd(x^3+x+2, x-1)? We've shown already above that $x^3+x+2=(x^2+x+2)(x-1) + 4$

Proceeding in the normal fashion in the Euclidean algorithm

$x^3+x+2=(x^2+x+2)(x-1) + 4$

gcd(x^3+x+2, x-1) = gcd(x-1,4)

and the greatest common divisor of any monomial and an integer is clearly 1, so x^3+x+2 and x-1 are coprime.

For a second example, consider gcd(x^2-1,x^2+2x+1)

$x^2+2x+1=\underline{(x^2-1)}*1+\underline{2x+2}$

$x^2-1=\underline{(2x+2)}*x/2+ \underline{-(x+1)}$

$2x+2=\underline{-(x+1)}*(-2)+\underline{0}$

Since factors of -1 make no difference, gcd(x^2-1,x^2+2x+1) is -(x+1)

Irreducibles

We've seen that x^3+x+2 and x-1 are coprime; they have no factors in common. So, are we able to determine "prime" polynomials? Indeed we can - depending on the field that the polynomial lies in. We call these *irreducibles* instead of primes.

Example

Take p(x)=$x^3 + x^2 + 2$ over $\mathbf{Z}_3$. Now we can factor this polynomial if it has a root - from the factor theorem (which also holds for polynomials over any commutative ring with identity) p(k)=0 means k is a root. So, let's look at the following: Since we're in $\mathbf{Z}_3$, we luckily only need to check three values p(0)=2 p(1)=1 p(2)=2 So we have p(x) having no roots - it is irreducible ("prime").

Now observe an interesting fact. Take the exact same polynomial but instead over $\mathbf{Z}_2$. The polynomial then is equivalent to

x^3+x^2+0

and thus has root p(0)=0 and thus *is reducible* but *over* $\mathbf{Z}_2$

So the reducibility of the polynomial depends on the field it is in.

Showing irreducibility

The general procedure to show a polynomial is irreducible is:

- observe its degree
- identify possible factorizations
- eliminate these factorizations

effectively a proof by cases.

For example, consider the polynomial q(x)=x^4+x+2 in $\mathbf{Z}_3$. To prove it is irreducible, observe that q(x) could be factorized in the following ways:

1. linear, irreducible cubic
2. linear, linear, irreducible quadratic

3. linear, linear, linear, linear
4. irreducible quadratic, irreducible quadratic

So we can prove 1, 2, 3 by showing it has no linear factors. 4 is a little more difficult. Let us proceed to show it has no linear factors: Observe

q(0)=2

q(1)=1

q(2)=2

So q has no linear factors. Now, we need to show that q is not the product of two irreducible quadratics.

In $\mathbf{Z}_3$, we have the quadratics

$\{x^2,x^2+1,x^2+x,x^2+x+1,x^2+x+2,x^2+2,x^2+2x,x^2+2x+1,x^2+2x+2\}$

We can identify the irreducible quadratics easily by inspection. We then obtain

$\{x^2+1,\ x^2+x+2,\ x^2+2x+2\}$

If we can show that neither of these polynomials divide $q(x)=x^4+x+2$, we have shown $q(x)$ is irreducible.

Let us try x^2+1 first.

$$\begin{array}{ccccccccc}
 & & & & & & 1 & 0 & 2 \\
1 & 0 & 1 & | & 1 & 0 & 0 & 1 & 2 \\
 & & & & 1 & 0 & 1 & & \\
 & & & & & & 2 & 1 & 2 \\
 & & & & & & 2 & 0 & 2 \\
 & & & & & & & 1 & 0
\end{array}$$

We have a remainder, so x^2+1 doesn't divide q. On dividing the other polynomials, we all get a remainder. (*Verify this for yourself as practice*).

So $q(x)$ is irreducible in $\mathbf{Z}_3$.

Modular arithmetic and polynomials

Since we have a working polynomial division and factor theorem, and that polynomials appear to mimic the behaviour of the integers - can we reasonably define some sort of modular arithmetic with polynomials?

We can indeed. If we have a field $\mathbf{Z}_p[x]$ and we wish to find all the remainders (remember, these remainders are polynomials) on dividing by some polynomial $m(x)$, we can do so by polynomial long division.

If $m(x)$ is irreducible, then the set of remainders as above forms a field.

Discrete Mathematics/Finite fields

Recall from the previous section that we considered the case where **F**[*x*]/<m("x")> analogous to modular arithmetic but with polynomials, and that when we are looking at numbers modulo *n*, we have a field iff $\mathbf{Z}_n$ is a field if *n* is prime.

Can we say something similar about **F**[*x*]/<m("x")>? Indeed, if m(*x*) is irreducible then **F**[*x*]/<m("x")> is a field.

This section deals with these kinds of fields, known as a **finite field**.

Definitions

We have the object **F**[*x*]/<m("x")> where this is the set of polynomials in **F**[*x*] are divided by the polynomial m(*x*).

Of the elements in **F**[*x*]/<m("x")> we can easily define addition, subtraction, multiplication, division and so on normally but with a reduction modulo m(*x*) to get the desired remainder.

We have that **F**[*x*]/<m("x")> is a commutative ring with identity, and if m(*x*) is irreducible then **F**[*x*]/<m("x")> is a field.

If m(*x*) has degree *n*, then

$$\mathbf{F}[x]/\text{<m("x")>}=\{a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+...+a_0\mathrm{x}^0|a_i\in\mathbf{F}\}$$

If **F** is $\mathbf{Z}_p$ (so *p* is prime) then |**F**[*x*]/<m("x")>|=p^n

Properties

Now remember with complex numbers **C**, we have "invented" the symbol i to stand for the root of the solution $x^2+1=0$. In fact, we have $\mathbf{C}=\mathbf{R}[x]/<x^2+1>$.

When we have a *general* finite field, we can do this also. We write this often as **F**[*x*]/<m("x")>=**F**(α) where α is "the root of" m(*x*) - we *define* α to be the root of m(*x*).

F(α) in fact is the smallest field which contains **F** and α.

Finite field theorems

We have a number of theorems associated with finite fields.

1. If **F** is a finite field, |**F**|=*q*, then $q=p^k$ for some $k \geq 1$ and *p* prime.
2. There then is a monic irreducible polynomial m(*x*) with degree *k* such that $\mathbf{F}=\mathbf{Z}_p[x]$/<m("x")>=$\mathbf{Z}_p(\alpha)$ with α a root of m(*x*) over $\mathbf{Z}_p$
3. There is an element γ∈**F** such that the order (the least element *n* such that $\gamma^n=1$) of γ is *q*-1, so γ is primitive in **F**, and we can generate elements of **F** (not zero) from powers of γ, i.e. $\mathbf{F}=\{0, \gamma^0=1, \gamma^1, ..., \gamma^{q-2}, \gamma^{q-1}=1\}$
4. **F** is a vector space with dimension *k* over $\mathbf{Z}_p$. It has basis $\{1, \alpha, \alpha^2,...,\alpha^{n-1}\}$ where *n* is the degree of m(*x*), so we have $\mathbf{F}=\{a_{n-1}\alpha^{n-1}+...+a_0\alpha^0|a_i\in\mathbf{F}\}$
5. If *a*∈F, *a*+...+*a* *p* times (*pa*) is 0.
6. If $m_2(x)$ is any other irreducible polynomial of degree *k* over $\mathbf{Z}_p$ then **F** is *isomorphic* (meaning basically equal to, except for a change in symbols) to $\mathbf{Z}_p/<m_2(x)>$ - so all ways of writing this field are basically the same. So there is essentially one field of size $q=p^k$ and we denote it GF(p^k) (GF meaning Galois Field).

Some examples

Let's look at a few examples that go through these ideas.

The complex numbers

Complex numbers, briefly, are numbers in the form

$$a + bi$$

where *i* is the solution to the equation $x^2+1=0$

These numbers in fact form a field, however it is not a finite field.

Take m(*x*)=x^2+1, with the field **F** being **R**. Then we can form the complex numbers as **F**/<m("x")>. Now **F**/<m("x")> = { *a*+*bx* | *a*, *b* ∈ **R**} because the remainders must be of degree less than m(*x*) - which is 2.

So then $(a+bx)(c+dx)=ac+bdx^2+(ad+bc)x$.

But remember that we are working in **F**/<m("x")>. So x^2 modulo x^2+1, can be written as $(x^2+1)-1=-1$, and substituting -1 above yields a rather familiar expression.

If we let the symbol *i* to be the "root of x^2+1", then $i^2+1=0$ and $i^2=-1$. The rest of the field axioms follow from here. We can then say the complex numbers **C**=**R**/<x^2+1>=**R**(*i*).

The $\mathbf{Z}_\mathbf{p}$ case

We can still do this for some field in general. Let's take $\mathbf{Z}_3$ for example, and pick m(*x*)=x^2+x+2. m(*x*) is irreducible - m(0)=2, m(1)=4=1, m(2)=4+2+2=8=2.

So $\mathbf{Z}_3$/<x^2+x+2> is a finite field. Assume α is a root of m(*x*). Then $\mathbf{Z}_3$(α) = { *a*+*b*α|*a*, *b* ∈ $\mathbf{Z}_3$}. Since $\mathbf{Z}_3$/<x^2+x+2> is finite, we can list out all its elements. We have the constant terms, then the α terms, then the α+constant terms, and so on. We have {0, 1, 2, α, α+1, α+2, 2α, 2α+1, 2α+2}.

Now we have $\alpha^2+\alpha+2=0$, then

$$\alpha^2=-\alpha-2$$

$$\alpha^2=2\alpha-2=2\alpha+1$$

(Recall the coefficients are in $\mathbf{Z}_3$! We are working in $\mathbf{Z}_3$/<m("x")>)

We can verify multiplication works mod m(*x*) - for example

$$(1+2\alpha)(2+\alpha) = 2 + \alpha+4\alpha+2\alpha^2$$

Reducing coefficients normally mod 3 we get

$$(1+2\alpha)(2+\alpha) = 2 + 2\alpha + 2\alpha^2$$

Now using the formula above for α^2

$$(1+2\alpha)(2+\alpha)$$

$$= 2 + 2\alpha + 2(2\alpha+1)$$

$$= 2 + 2\alpha+4\alpha+2$$

$$= 2 + 6\alpha+2$$

$$= 2 + 2 = 4 = 1$$

Verify for yourself that multiplication and other operations work too.

Primitive elements

Recall from ../Modular arithmetic/ that the order of a number a modulo n, in a field, is the least power such that $a^{k\text{-}1}$=1 in $\mathbf{Z}_n$, with k the size of this field. Since the order is defined over a field, this leads us to consider whether we have primitive elements in **F**[x]/<m("x")> - which we do. If we have **F**(α), just like in $\mathbf{Z}_n$, α is primitive iff the order of α is q-1 where q is the number of elements in **F**[x]/<m("x")>.

Let's take $\mathbf{Z}_2$/<x^2+x+1>. Is α (root of x^2+x+1) primitive?

First, if α is a root of x^2+x+1,

α^2+α+1=0

α^2=-α-1=α+1

Now, let us calculate powers of α

1, α

α^2=α+1

α^3=α(α^2)=α(α+1)=α^2+α=(α+1)+α=1

Recall that the size of this field is 4 (the n in $\mathbf{Z}_n$, in this case, 2, raised to the power of the degree of the polynomial, in this case 2). Now we have α^3=$\alpha^{4\text{-}1}$=1, and α is primitive.

We generally want to look at powers of α in **F**(α), to see whether they are primitive, since we already know about the orders of the constants in **F**(α) - which we've looked at in ../Modular arithmetic/.

Discrete Mathematics/Arithmetic Functions

An **arithmetic function** is a function from the set of positive integers to the set of complex numbers. Examples of important arithmetic functions include:

The Euler totient function, φ(n) defined to be the number of positive integers less than and relatively prime to n

The Mobius function, $\mu(n) = \begin{cases} 1, & \text{if } n \text{ is square free with an even number of prime factors} \\ -1, & \text{if } n \text{ is square free with an odd number of prime factors} \\ 0 & \text{otherwise} \end{cases}$

$$e(n) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{otherwise} \end{cases}$$

The Von Mangoldt function, $\Lambda(n) = \begin{cases} \ln p, & \text{if } n = p^k \text{ for some prime} p \text{and} k \geq 1 \\ 0, & \text{otherwise} \end{cases}$

$$\sigma_k(n) = \sum_{d|n} d^k$$

and

$$\theta_k(n) = n^k$$

Many of these functions are multiplicative that is they satisfy a(m)a(n)=a(mn) when m and n are relatively prime. A function that satisfies a(m)a(n)=a(mn) even when m & n are not relatively prime is called completely multiplicative. To define a multiplicative function, a(n), it suffices to only give its values when n is the power of a prime; For a completely multiplicative function, giving its values when n is prime uniquely defines the function.

Given 2 arithmetic functions their Dirichlet convolution is defined by

$$(a*b)(n)=\sum_{d|n}a(d)b(\frac{n}{d})$$

where the sum is taken over the divisors, d, of n. It is easy to show that

$$(a*e)(n)=a(n),$$

that is the function e(n) is the identity under Dirichlet convolution. Another basic fact is that Dirichlet convolution is commutative and associative.

It is also straightfoward to show that multiplicative functions form a group under Dirichlet convolution, or in other words, the following properties hold in addition to the fact that e(n) is the identity, and its associativity:

- for any multiplicative function a there is a multiplicative function b such that (a * b) = e

and

- the Dirichlet convolution of 2 multiplicative functions is also multiplicative.

The most important fact about the Von Mangoldt function is that

$$\sum_{d|n}\Lambda(n)=\ln n.$$

The Mobius function's significance comes from the fact that

$$\sum_{d|n}\mu(n)=e(n),$$

and thus if $f(n)=\sum_{d|n}g(d)$then $g(n)=\sum_{d|n}f(d)\mu(\frac{n}{d})$.

Discrete Mathematics/Analytic Number Theory

Analytic Number Theory is the application of Analysis to Number Theoretic Problems. A quick overview of some portions of Analytic Number theory follow.

Zeta function

The zeta function defined by

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s}$$

for real values of s > 1, plays a central role in the theory. It is straightfoward to show it converges absolutely when s > 1. It satisfies the Euler product formula,

$$\zeta(s)=\prod_p\frac{1}{1-p^{-s}}$$

where the product is over all prime numbers. To see this note that multiplying the series definition by $1-2^{-s}$ and rearranging terms(which is justified since the series converges absolutely) eliminates the even terms, i.e. $(1-2^{-s})(1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\ldots)=(1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\ldots)-(\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{6^s}+\frac{1}{8^s}+\frac{1}{10^s}+\ldots)=(1+\frac{1}{3^s}+\frac{1}{5^s}+\frac{1}{7^s}+\ldots)$

Likewise after multiplying by $1-3^{-s}$ all remaining terms with n divisible by 3 are eliminated. After repeating this process for all primes it follows that

$$\zeta(s)\prod_p\left(1-p^{-s}\right)=1$$

since 1 is the only number not divisible by a prime and thus only the n=1 term is left. Solving for ζ(s) immediately gives the Euler product formula.

Dirichlet series

The series for the zeta function is a special case of a Dirichlet series, that is a series of the form

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

Many important arithmetic functions, a(n), have the properties that a(1)=1 and a(m)a(n)=a(mn) when m & n are relatively prime. Such functions are called multiplicative and their associated Dirichlet series may be expressed as an Euler product by

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p} \sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}},$$

as can be shown in a manner similar to the proof for the zeta function. A completely multiplicative function is one where a(m)a(n)=a(mn) even if m & n are not relatively prime. For a completely multiplicative function, the Euler product simplifies to

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p} \frac{a(p)}{1-p^{-s}}.$$

The product of two Dirichlet series is given by the formula

$$\left(\sum_{k=1}^{\infty} \frac{a(k)}{k^s}\right)\left(\sum_{m=1}^{\infty} \frac{b(m)}{m^s}\right) = \sum_{n=1}^{\infty} \frac{(a*b)(n)}{n^s}$$

where (a * b)(n) represents the Dirichlet convolution of a & b, which is defined by

$$(a*b)(n) = \sum_{d|n} a(d) b\left(\frac{n}{d}\right)$$

Some important Dirichlet series include:

$$\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

$$\zeta(s-k) = \sum_{n=1}^{\infty} \frac{n^k}{n^s}$$

and

$$\zeta(s)\zeta(s-k) = \sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s}$$

Big-Oh notation

Many problems involve functions that are incredibly difficult to work with exactly, but where the rate of growth of the function, rather than its exact values, is of primary concern. Because of this a notation (often called "Big-Oh notation") was invented.

"f(x)=O(g(x))" is used to denote that for a sufficiently large number x_0 there exists a number C such that for all $x>x_0$

$$|f(x)| \leq Cg(x)$$

"f(x) = g(x) + O(h(x))" is used to denote that f(x)-g(x)=O(h(x))

Dirichlet's Theorem

One of the first results proven with analytic number theory was Dirichlet's Theorem which states that for any 2 relatively prime integers a & b, there are infinitely many values of k for which ak+b is a prime number. The proof involves complex-valued functions of the set of integers called Dirichlet characters defined by the properties that χ(n) depends only on its residue class modulo a, χ(n) is completely multiplicative, and χ(n) = 0 iff a and n are not relatively prime. The principal character χ_0 is defined to be 1 when a & n are relatively prime and 0 otherwise. It is easy to show that χ_0 is a character. It can be shown that the number of characters is equal to φ(a). It can also be shown that the sum of the values of χ(n) over all characters χ is equal to φ(a) if $n \equiv 1 \pmod{a}$and 0 otherwise. The Dirichlet series corresponding to a character is called a Dirichlet L-series and is traditionally denoted by L(s,χ). It is simple to show that $L(1,\chi_0)$ diverges. Through a complicated argument it is shown that L(1,χ) converges and is nonzero if χ is nonprincipal. The function

$$\sum_{p\equiv b \pmod{a}} \frac{1}{p} = \sum_{\chi} \frac{L(1,\chi)}{\chi(b)} + O(1)$$

must diverge since $L(1,\chi_0)/\chi(b)$ diverges and the other terms all converge. Since all terms of the sum on the left are finite its divergence implies there are an infinite number of terms of this sum and thus infinitely many primes of the form ak+b.

Riemann zeta function & xi function

The zeta function introduced above(the Euler zeta function) converges for all values of s such that Re(s)>1. The Riemann zeta function is defined as the analytic continuation of the Euler zeta function, and is defined for all complex values of s except s=1. Where both functions exist, the Euler and Riemann zeta functions are equal by definition. It can be shown that if the xi function is defined by

$$\xi(s) = \frac{1}{2}s(s-1)\Gamma(\frac{s}{2})\pi^{-\frac{s}{2}}\zeta(s)$$

then ξ(s)=ξ(1-s). This is the symmetric form of the famous functional equation for the Riemann zeta function, and provides a convenient way of computing the Riemann zeta function when Re(s)<1.

The series definition of Euler's zeta function shows that ζ(s) has no zeroes for Re(s)>1. It can also be shown that the zeta function has no zeroes with Re(s)=1. The functional equation shows that for integer values of n, ζ(-2n)=0, and any other zeroes lie in the so-called critical strip, 0<Re(s)<1. The well-known Riemann Hypothesis states that all nontrivial zeros(i.e. those not of the form s=-2n), have Re(s)=1/2. It is easy to show that the zeroes of the xi function are exactly the nontrivial zeroes of the zeta function.

Hadamard product formula

The Hadamard product formula states that functions with certain properties(in particular the xi function) are close enough to a polynomial that they may be represented in terms of a product over the zeroes. For the xi function the Hadamard product formula states that

$$\xi(s) = e^{A+Bs}\prod_{\rho}(1-\frac{s}{\rho})$$

for certain values of A and B, where the product is over the zeroes of ξ(s). This formula is one of the main reasons the zeroes of the xi function, and thus the zeta function, are of considerable importance.

Distribution of squarefree numbers

Let S(x) denote the number of squarefree numbers less than or equal to x. To evaluate this function we begin by counting all integers less than or equal to x. Then we subtract those that are divisible by 4, those divisible by 9, those divisible by 25, and so on. We then have removed numbers with 2 repeated prime factors twice those with 3 repeated prime factors 3 times and so on. To remedy the repetition of the numbers with 2 repeated prime factors we add on the number of integers less than or equal to x divisible by 36, those divisble by 100, those divisible by 225 and so on. We have now reincluded those with 3 repeated prime factors so we uncount them. Continuing this process gives

$$S(x) = \sum_{n^2 \leq x} \mu(n) \left\lfloor \frac{x}{n^2} \right\rfloor = \sum_{n^2 \leq x} \mu(n) \frac{x}{n^2} + O(\sqrt{x}) = \frac{x}{\zeta(2)} + O(\sqrt{x}) = \frac{6}{\pi^2} x + O(\sqrt{x})$$

In addition to information about how common squarefree numbers are this estimate gives information on how they are distributed. For example to show that there are infinitely many pairs of consecutive squarefree numbers(i.e. that differ by 1) assume there are only finitely many such pairs. Then there is some x_0 such that all such pairs lie below x_0. Then for n > x_0 n and n+1 cannot be squarefree, and thus at most half the integers above x_0 are squarefree, or more precisely,

$$S(x) \leq \frac{1}{2}(x - x_0) + x_0 + 1 = \frac{x}{2} + O(1)$$

but since $\frac{6}{\pi^2} > \frac{1}{2}$this contradicts the estimate obtained earlier, thus there are infinitely many pairs of consecutive squarefree numbers.

The estimate also shows that for large enough x, there is at least one squarefree number between x^3 and (x+1)^3. To see this not that the number of squarefree numbers in that range is

$$S\left((x+1)^3\right) - S(x^3) = \frac{6}{\pi^2}\left((x+1)^3 - x^3\right) + O\left(\sqrt{(x+1)^3}\right) + O\left(\sqrt{x^3}\right) = \frac{18}{\pi^2} x^2 + O\left(x^{\frac{3}{2}}\right)$$

which is at least one for sufficiently large x.

To do: Add mention of prime number theorem and sieve methods, as well as Dirichlet inversion

Abstract Algebra/Group Theory

This book is on *abstract algebra* (abstract algebraic systems), an advanced set of topics related to algebra, including groups, rings, ideals, fields, and more. Readers of this book are expected to have read and understand the information presented in the Algebra, and Linear Algebra books.

Contents

This book is part of a series on **Algebra:**

Basic Algebra
Algebra
Intermediate Algebra
Linear Algebra
Abstract Algebra
Intro to Rings and Algebras

1. Introduction
    1. Sets
    2. Equivalence relations and congruence classes
    3. Functions
    4. Binary Operations
    5. Linear Algebra
    6. Number Theory
2. Group Theory
    1. Reasons to Write or Read This
    2. Groups
    3. Subgroups
    4. Cyclic groups
    5. Permutation groups
    6. Homomorphism
    7. Normal subgroups and Quotient groups
    8. Free groups
    9. Group actions on sets
    10. The Sylow Theorems
    11. Group tables
3. Rings
    1. Rings
    2. Ring Homomorphisms
    3. Ideals
    4. Integral domains
    5. Fraction Fields
    6. Polynomial Rings
4. Fields
    1. Fields
    2. Factorization
    3. Splitting Fields and Algebraic Closues
    4. Separability, Normal Extensions

5. Vector Spaces
    1. Vector Spaces
6. Modules
    1. Modules
    2. Hypercomplex numbers
7. Algebras
    1. Algebras
    2. Boolean algebra
    3. Clifford Algebras
    4. Quaternions
    5. Galois Theory
8. Further abstract algebra
    1. Category theory
    2. Lattice theory
    3. Matroids
9. Authors

Related books

- See Subject:Algebra

Information for contributors

- Manual of Style

Not a book title page. Please remove from this page.

Abstract Algebra/Lattice theory

A *lattice* is a *poset* such that each pair of elements has a unique *least upper bound* and a unique *greatest lower bound*.

Abstract Algebra/Matroids

A matroid is an algebraic construct that is related to the notion of independence.

Matroids are an abstraction of several combinatorial objects, among them graphs and matrices. The word matroid was coined by Whitney in 1935 in his landmark paper "On the abstract properties of linear dependence". In defining a matroid Whitney tried to capture the fundamental properties of dependence that are common to graphs and matrices. Almost simultaneously, Birkhoff showed that a matroid can be interpreted as a geometric lattice. Maclane showed that matroids have a geometric representation in terms of points, lines, planes, dimension 3 spaces etc. Often the term combinatorial geometry is used instead of simple matroids. However, combinatorial geometry has another meaning in mathematical literature. Rank 3 combinatorial geometries are frequently called linear spaces. Matroids are a unifying concept in which some problems in graph theory, design theory, coding theory, and combinatorial optimization become simpler to understand.

Abstract Algebra/Category theory

Category theory is the study of *categories*, which are collections of objects and *morphisms* (or arrows), or from one object to another. See Category Theory for additional information.

Definitions & Notations

A *category* consists of a class G of *objects* and for every pair of objects A, B in G a class $Hom(A, B)$ of things called *morphisms* or *arrows* from A to B. This may be thought of as a *directed graph* where G are the points and $Hom(A, B)$ are the directed lines between them.

For every three objects A, B and C in G there is a map o called composition:

$o : Hom(A, B) \times Hom(B, C) \rightarrow Hom(A, C)$

We write $f \circ g$ for the composition of f and g

Composition is associative, i.e. for and A, B, C, D in G, for any f in $Hom(A, B)$, g in $Hom(B, C)$, h in $Hom(C, D)$,

$(f \circ g) \circ h = f \circ (g \circ h)$

For every object A in the category there is a special map i_A in $Hom(A, A)$ which we call the *identity* of A. This has the properties:

for any object B in G, any g in $Hom(A, B)$, $i_A \circ g = g$

for any object B in G, any h in $Hom(B, A)$, $h \circ i_A = h$

[Note if j_A is another identity for A, the axioms imply that

$j_A = j_A \circ i_A = i_A$,

so the identity for each object is unique.]

Some examples of categories

- $\mathbf{Set}$, the category whose objects are sets, and whose morphisms are maps between the sets.
- The category whose objects are open subsets of $\mathbb{R}^n$ and whose morphisms are continuous (differentiable, smooth) maps between them.
- The category whose objects are smooth (differentiable,topological) manifolds, and morphisms are smooth (differentiable,continuous) maps.
- $k-\mathbf{Vect}$, the category whose objects are vector spaces over a field k (for example, the real or complex numbers), with morphisms linear maps.
- $\mathbf{Group}$, the category of groups, and homomorphisms between them.

In all the examples I have given thus far, the objects have been sets with the morphisms given by set maps between them. This is not always the case. There are some categories where this is not possible, and others where the category doesn't naturally appear in this way. For example:

- Let $\mathcal{G}$ be any category. Then its opposite category $\mathcal{G}^{op}$ is a category with the same objects, and all the arrows reversed. More formally, a morphism in $\mathcal{G}^{op}$ from an object X to Y is a morphism from Y to X in $\mathcal{G}$.
- Let G be any group. Then we can define a category with a single object, with morphisms from that object to itself given by elements of G with composition given by multiplication in G.

Abstract Algebra/Hypercomplex numbers

Hypercomplex numbers are numbers that use the square root of -1 to create more than 1 extra dimension.

The most basic Hypercomplex number is the one used most often in vector mathematics, the Quaternion, which consists of 4 dimensions. Higher dimensions are diagrammed by adding more roots to negative 1 in a predefined relationship.

Quaternions

A Quaternion consists of four dimensions, one real and the other 3 imaginary. The imaginary dimensions are represented as *i*, *j* and *k*. Each imaginary dimension is a square root of -1 and thus it is not on the normal number line. In practice, the *i*, *j* and *k* are all orthogonal to each other and to the real numbers. As such, they only intersect at the origin (0,0*i*, 0*j*, 0*k*).

The basic form of a quaternion is:

- $q = a + bi + cj + dk$

where a, b, c and d are real number coefficients.

For a quaternion the relationship between *i*, *j* and *k* is defined in this simple rule:

- $i^2 = j^2 = k^2 = i \times j \times k = -1$

From this follows:

- $i \times j = k$, $j \times i = -k$
- $j \times k = i$, $k \times j = -i$
- $k \times i = j$, $i \times k = -j$

As you may have noticed, multiplication is not commutative in hyperdimensional mathematics.

They can also be represented as a 1 by 4 matrix in the form

real	***i***	***j***	***k***

1	1	1	1

...

...

The quaternion is a 4 dimensional number, but it can be used to diagram three dimensional vectors and can be used to turn them without the use of calculus.

see also: Wikipedia's Article on Quaternion [1]

Octonion

8-dimensional. See: Wikipedia's Article on Octonion [2]

Sedenions

16-dimensional. See: Wikipedia's Article on Sedenion [3]

References

[1] http://en.wikipedia.org/wiki/Quaternion
[2] http://en.wikipedia.org/wiki/Octonion
[3] http://en.wikipedia.org/wiki/Sedenion

Abstract Algebra/Rings

Introduction to Rings

Rings are algebraic structures designed to model and abstract the structure of the integers ($\mathbb{Z}$), so that we can duplicate some of the processes in which integers are used, but in a more general setting. It will be helpful if you have familiarity with the concepts and theorems for groups, because we'll be using many of the same ideas and theorems.

Definition: A *ring* is a set R with two binary operations $+$ and $\cdot$ that satisfies the following properties:

For all $a, b, c \in R$,

1. $(R, +)$ is an abelian group:
    1. $a + b \in R$ (R is closed under $+$)
    2. $(a + b) + c = a + (b + c)$ ($+$ is associative)
    3. $\exists 0 \in R : 0 + a = a$ (R contains an additive identity)
    4. $\exists - a \in R : a + (-a) = 0$ (R contains additive inverses)
    5. $a + b = b + a$ ($+$ is commutative)
2. $(R, \cdot)$ is a semigroup:
    1. $a \cdot b \in R$ (R is closed under $\cdot$)
    2. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ ($\cdot$ is associative)
3. $\cdot$ is distributive over $+$:
    1. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
    2. $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$

We'll often use juxtaposition in place of $\cdot$, i.e., ab for $a \cdot b$.

Examples

1. The set $\mathbb{Z}$ of integers under standard addition and multiplication.
2. The set $2\mathbb{Z}$ of even integers under standard addition and multiplication.
3. The sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are also rings under standard addition and multiplication.
4. The set $M_2(\mathbb{R})$ of 2x2 square matrices with real coefficients under standard addition and multiplication.
5. The set $Maps(\mathbb{R},\mathbb{R})$ of functions on $\mathbb{R}$ with pointwise addition and multiplication.
6. More generally, if R is a ring, the set $Maps(R,R)$ is also a ring.
7. The set $Maps(R,R)$ with function composition for multiplication is **not** a ring since the statement $f\circ(g+h)=f\circ g+f\circ h$ is not true in general.
8. The set of integrable functions on the real numbers, L^1, is a ring under pointwise addition and multiplication given by *convolution*:

$$(f*g)(t)=\int_{\mathbb{R}}f(\tau)g(t-\tau)d\tau$$

This ring is important to the study of linear systems and differential equations.

1. The set $\{0\}$ with the only possible binary operations is called the *trivial* ring or the *zero* ring. As we will see, all singleton sets are isomorphic to $\{0\}$ when given operations. A ring which contains more than one element is called a **non-zero ring**.
2. The set of Gaussian integers $\mathbb{Z}\left[i\right]=\{a+bi|a,b\in\mathbb{Z}\}$ with standard addition and multiplication.
3. Let R be a ring, and let R[X] denote all the polynomials $a_nX^n+a_{n-1}X^{n-1}+...+a_1X+a_0$with coefficients in R. Then R[x] is a ring under standard addition and multiplication. If $f(x)=\sum_{i=0}^{m}a_ix^i$ and $g(x)=\sum_{i=0}^{n}b_ix^i$, then $(fg)(x)=\sum_{i=0}^{m+n}c_ix^i$ where $c_i=\sum_{j=0}^{i}a_jb_{i-j}$. Polynomial multiplication is also called *discrete convolution*.

Theorem: Let R be a ring, and let $a,b,c\in R$. Then the following are true:

1. If $a+b=a+c$, then $b=c$.
2. The equation $a+x=b$ has a unique solution.
3. $-(-a)=a$
4. $0a=0$
5. $(-a)b=-(ab)$
6. $(-a)(-b)=ab$

Proof: (1), (2), and (3) all strictly concern addition, and are all previous results from $(R,+)$being a group. The other three parts all concern both addition and multiplication (since 0 and - are additive concepts), so as a proof strategy we expect to use the distributive law in some way to link the two operations. For (4), observe that 0a + 0a = (0 + 0)a = 0a. But then by (1), a=0. For (5), Note that (-a)b + ab = (-a + a)b = 0b = 0. For (6) note that (-a)(-b) + -(ab) = (-a)(-b) + (-a)b = -a(-b + b) = -a0 = 0.

Types of Rings

Definition: Note that a ring does not necessarily have the property of commutative multiplication. When it does, the ring is called a *commutative ring*.

Definition: Also, a ring does not necessarily have a multiplicative identity. A nonzero element of a ring that is an identity under multiplication is sometimes called *unity* and is denoted 1. Rings that contain a multiplicative identity are called *rings with unity*.

Examples

1. $\mathbb{Z}$ is a commutative ring with 1.
2. $M_2(\mathbb{R})$ is a non-commutative ring with $1 = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
3. $2\mathbb{Z}$ is a commutative ring without 1.
4. As a more complicated example, L^1 with convolution is also a commutative ring without 1.

Exercise: Prove that in any ring with 1, the multiplicative identity is unique.

Exercise: As noted earlier, there is a single trivial or zero ring. Show that a ring with unity R is the trivial ring if and only if $1 = 0$.

Definition: Let R be a ring with 1. An element $r \in R$ is a *unit* and is *invertible* if there is an element $r^{-1} \in R$ such that $rr^{-1} = 1$. The set of all units is denoted by $R^\star$.

Exercise: Prove that $R^\star$ is a group under multiplication.

Definition: An non-zero element $r \in R$ is a *zero-divisor* when there exists a nonzero $s \in R$ such that rs = 0.

Exercise: Show that a zero-divisor is not a unit.

Definition: A commutative ring R with a $1 \neq 0$ and no zero-divisors is called an *integral domain.*

Integral domains are modeled after $\mathbb{Z}$, which is where they get their name. They are often very nice rings to work in due to the following theorem:

Theorem (Cancellation Law for Integral Domains): Let R be an integral domain, and let $a, b, c \in R$ be nonzero. Then $ab = ac$ if and only if $b = c$.

Proof: Evidently $ab = ac$ if $b = c$. To see the other direction, we rearrange the equality as $ab - ac = 0$. But then $a(b - c) = 0$. Since a is nonzero, and R contains no zero divisors, it must be the case that $b - c = 0$, which is to say that $b = c$.

Definition: A ring R with a $1 \neq 0$ is a *division ring* or *skew field* if all non-zero elements are units i. e. under multiplication, it forms a group with its nonzero elements.

Definition: A field is a commutative division ring. Alternatively, a field F is a ring where $(F, \cdot)$ is an abelian group. As another alternative, a field is an integral domain where all non-zero elements are invertible.

As stated before, integral domains are easy to work with because they are so close to being fields. In fact, the next theorem shows just how close the two are:

Theorem: Let R be a finite integral domain. Then R is a field.

Proof: Let $a \in R$ be nonzero and let $S = \{ab | b \in R\}$. Clearly S is a subset of R . From the cancellation law, we can see that $|S| = |R|$ (since if two elements ab and ac are equal, then $b = c$). But then $S = R$. So then there must be some b such that $ab = 1$. So a is a unit.

Of course proving that a set with two operations satisfy all of the ring axioms can be tedious. So, just as we did for groups, we note that if we're considering a subset of something that's already a ring, then our job is easier.

Definition: A *subring* S of a ring R is a subset of R that is also a ring (under the same two operations as for R). We denote " S is a subring of R " by $S \leq R$.

Theorem: Let S be a subset of a ring R . Then $S \leq R$ iff:

1. S is nonempty
2. S is closed under $+$
3. $\forall a \in S$, $-a \in S$
4. S is closed under $\cdot$

Examples:

1. $2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.

2. The trivial ring $\{0\}$ is a subring of every ring.
3. The set of Gaussian integers $\mathbb{Z}[i]$ is a subring of the complex numbers $\mathbb{C}$.
4. Let R be a ring, and consider the set of polynomials, $R[x]$. Then the set of constant polynomials $S = \{a_0 | a_0 \in R\}$ is a subring of $R[x]$. Note that the elements of R and the constant polynomials in $R[x]$ are *not* the same objects. However, we can see how we might regard R as a subring of $R[x]$ anyway. We will make this idea more precise when we study homomorphisms in the next section.

Discrete Mathematics/Combinatory logic

Two of the basic principles of combinatory logic in discrete mathematics are the Sum principle and the Multiplication principle.

The sum principle holds true in a given partitioned set X where partition Xi intersected with Xj is the empty set unless i is equal to j. The principle states that in such a partitioned set, the sum of the elements of each partition is equal to the number of elements in the set X.

Discrete Mathematics/Finite state automata

Formally, a Deterministc Finite Automaton is a 5-tuple $D = (Q, \Sigma, \delta, s, F)$ where:
Q is the set of all states.
$\sum$is the alphabet being considered.
δ is the set of transitions, including exactly one transition per element of the alphabet per state.
s is the single starting state.
F is the set of all accepting states.

Similarly, the formal definition of a Nondeterministic Finite Automaton is a 5-tuple $N = (Q, \Sigma, \delta, s, F)$ where:
Q is the set of all states.
$\sum$is the alphabet being considered.
δ is the set of transitions, with epsilon transitions and any number of transitions for any particular input on every state.
s is the single starting state.
F is the set of all accepting states.

Note that for both a NFA and a DFA, s is not a set of states. Rather, it is a single state, as neither can begin at more than one state. However, a NFA can achieve similar function by adding a new starting state and epsilon-transitioning to all desired starting states.

The difference between a DFA and an NFA being the delta-transitions are allowed to contain epsilon-jumps(transitions on no input), unions of transitions on the same input, and no transition for any elements in the alphabet.

For any NFA N, there exists a DFA D such that $L(N) = L(D)$

Discrete Mathematics/Selected problems

The problems in the texts you have seen are for you to ensure that you understand the concepts and ideas explored. They are not intended to be very difficult, but understandably they are not very challenging.

Questions here are intended for you to further use the ideas you have learnt to answer some more difficult questions. Some questions are relatively straightforward, some of these questions depend on different sections of this discrete mathematics text, some of these questions are meant to be examination-style questions.

Do not be discouraged by the increase in difficulty - hints are sometimes available, and you will be able to increase your problem solving skills!

Set theory questions

These questions depend on your knowledge of ../Set theory/.

1. We have the sets A={0, 1, 3, 4, 5, 7}, B = {2, 4, 5, 8, 9}, C = {1, 4, 9, 11, 21}. Write the elements of the set $(A \cap C) \cup B$ Check your solution: [1]
2. Using the set identities, simplify $(A \cap B)' \cup A$
3. (Hint provided) Prove the set $\{x|x/2 \in \mathbb{N}\}$ is not a subset of $\{y|y/4 \in \mathbb{N}\}$
4. (Hint provided) Prove the set $\{3n+5|n \in \mathbb{N}\}$ is not a subset of $\{6k+6|k \in \mathbb{N}\}$

References

[1] http://de.geocities.com/hasslerkun/SolutionCheckerEN.html?hv=96562c918a&no=1

Discrete Mathematics/Axiom of choice

Axiom of choice:

If $f : A \longrightarrow B$ is a surjective map, then there exists a map $g : B \longrightarrow A$ such that $f \circ g$ is the identity (trivial) map.
Lemma: Every set can be well-ordered.

Discrete Mathematics/Naive set theory

When we talk of **set theory**, we generally talk about *collections* of certain mathematical objects. In this sense, a *set* can be likened to a bag, holding a finite (or conceivably infinite) amount of things. Sets can be sets of sets as well (bags with bags in them). However, a set cannot contain duplicates -- a set can contain only one copy of a particular item.

When we look at sets of certain types of numbers, for example, the natural numbers, or the rational numbers, for instance, we may want to speak only of these sets. These collections of numbers are, of course, very important, so we write special symbols to signify them.

We write sets in curly brackets -- { and }. We write all of the *elements*, or what the set contains, in the brackets, separated by commas. We generally denote sets using capital letters.

For example, we write the set containing the number 0 and the number 1 as {0,1}. If we wish to give it a name, we can say B={0,1}.

Special sets

The aforementioned collections of numbers, the naturals, rationals, etc. are notated as the following:

- the *natural* numbers are written $\mathbb{N}$

  {0,1,2,...}
- the *integers* are written $\mathbb{Z}$

  {0,1,-1,2,-2,...}
- the *rational* numbers are written $\mathbb{Q}$

  {0,1,1/2,1/3,...,2,2/3,2/4,...}
- the *real* numbers are written $\mathbb{R}$

  {0, $-\sqrt{2}$, $\sqrt{2}$, π ,...}

Here we will generally write these in standard face bold instead of the doublestruck bold you see above. So we write here **N** instead of $\mathbb{N}$ (NB following Wikipedia conventions).

Notations

We can write some special relations involving sets using some symbols.

Containment relations

To say that an element is in a set, for example, 3 is in the set {1,2,3}, we write:

$$3 \in \{1,2,3\}$$

We can also express this relationship in another way: we say that 3 is a *member* of the set {1,2,3}. Also, we can say the set {1,2,3} *contains* 3, but this usage is not recommended as it is also used to refer to subsets (see following).

We can say that two sets are equal if they contain exactly the same elements. For example, the sets {2,3,1} and {3,1,2} both contain the numbers 1, 2 and 3. We write:

$$\{2,3,1\} = \{3,1,2\}$$

We write the set with *no* elements as $\emptyset$, or {}. Here, we use the notation {} for the *empty set* (NB following Wikipedia conventions).

The concept of the subset

A very important concept in set theory and other mathematical areas is the concept of the **subset**.

Say we have two sets A={0,1,2,3,4,5,6,7,8,9}, and B={0,1,2,3,4,5}. Now, B *contains some elements* of A, but not all. We express this relationship between the sets A and B by saying B is a *subset* of A. We write this

$$B \subseteq A$$

If B is a subset of A, but A is not a subset of B, B is said to be a *proper subset* of A. We write this

$$B \subset A$$

Note that if $B \subset A$, then $B \subseteq A$

Intersections and unions

There are two notable and fundamental special operations on sets, the *intersection* and the *union*. These are somewhat analogous to multiplication and addition.

Intersection

The intersection of two sets A and B are the elements *common* to both sets. For example, if A={1,3,5,7,9} and B={0,1,3}, their intersection, written $A \cap B$ is the set {1,3}.

If the intersection of any two sets are empty, we say these sets are *disjoint*.

Unions

The union of two sets A and B are the *all* elements in *both* sets. For example if A={1,3,5,7,9} and B={0,2,4,6,8}. We say the union, written $A \cup B$ is the set {0,1,2,3,4,5,6,7,8,9}.

Set comprehensions

When we write a set, we can do so by writing all the elements in that set as above. However if we wish to write an *infinite* set, then writing out the elements can be too unwieldy. We can solve this problem by writing sets in *set comprehension* notation. We do this by writing these sets including a *rule* and by a relationship to an *index set*, say I. That is;

$$S = \{x \in I | rule\}$$

where rule can be something like x^2, or x=3x.

For example, this set forms the set of all even numbers:

$$\{x \in \mathbb{N} | x \mod 2 = 0\}$$

This set forms the set of all solutions to the general quadratic:

$$\{x \in \mathbb{C} | ax^2 + bx + c = 0\}$$

Universal sets and complements

Universal sets

When we do work with sets, it is useful to think of a larger set in which to work with. For example, if we are talking about sets {-1,0,1} and {-3,-1,1,3}, we may want to work in **Z** in this circumstance. When we talk about working in such a larger set, such as **Z** in that instance, we say that **Z** is a *universal set*, and we take all sets to be subsets of this universal set.

We write the universal set to be $\mathcal{E}$, however it may be simpler to denote this as **E**.

Complements

Given a set A in a larger universal set **E**, we define the complement of A to be all elements in E that are not in A, that is the complement of A is:

$$\{x \in \mathcal{E} | x \notin A\}$$

We write the complement as A' or A^{c}. In this document we will use A'.

Problem set

Based on the above information, write the answers to the following questions (Answers follow to even numbered questions)

1. Is $3/4 \in \mathbb{Q}$?
2. Is $\sqrt{2} \in \mathbb{Q}$?
3. Is $\{x \in \mathbb{N} | 2x\} = \{x \in \mathbb{N} | \frac{x}{2} \in \mathbb{N}\}$?
4. True or false? If false, give an example of an element in the first set which is not in the second.
   1. $\mathbb{N} \subset \mathbb{Z}$
   2. $\mathbb{Q} \subset \mathbb{Z}$
5. True or false? If false, give an example of an element in the first set which is not in the second.
   1. $\mathbb{R} \subset \mathbb{Q}$
   2. $\mathbb{Z} \subset \mathbb{R}$
6. Is $\{1, 2, 3\} \subset \{1, 2, 3, 4\}$?
7. Is $\{1, 2, 3, 5\} \subseteq \{1, 2, 3, 4\}$?
8. Write the 5 elements of
   $\{x \in \mathbb{Z} | x - 3 \mod 2 = 0\}$
9. Write the elements of
   $\{x \in \mathbb{C} | x^2 + 4x - 3 = 0\}$
10. Find a universal set such that these sets are subsets thereof:
    $\{x \in \mathbb{Z}^{+} | a = x^2 and \sqrt{a} \in \mathbb{N}\}, \{x \in \mathbb{N} | x/3\}$
11. Given $\mathcal{E} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, find A' given $A = 1, 4, 7, 9$

Answers

2. No, the square root of 2 is *irrational*, not a rational number

4.1. Yes

4.2. No

6. Yes.

8. 5 elements could be {3,5,7,9,11}.

10. $\mathcal{E} = \mathbb{Q}$

Further ideas

These mentioned concepts are not the only ones we can give to set theory. Key ideas that are not necessarily given much detail in this elementary course in set theory but later in abstract algebra and other fields, so it is important to take a grasp on these ideas now.

These may be skipped.

Power set

The *power set*, denoted P(S), is the set of *all* subsets of S. ***NB***: The empty set is a subset of **all** sets.

For example, P({0,1})=

Cardinality

The *cardinality* of a set, denoted |S| is the amount of elements a set has. So |{a,b,c,d}|=4, and so on. The cardinality of a set need not be finite: some sets have infinite cardinality.

The cardinality of the power set

If P(S)=T, then |T|=$2^{|S|}$.

Problem set

Based on the above information, write the answers to the following questions. (Answers follow to even numbered questions)

1. |{1,2,3,4,5,6,7,8,9,0}|
2. |P({1,2,3})|
3. P({0,1,2})
4. P({1})

Answers

2. 2^3=8
4.

Set identities

When we spoke of the two fundamental operators on sets before, that of the *union* and the *intersection*, we have a set of rules which we can use to simplify expressions involving sets. For example, given:

$$(A \cup B)' \cap B' \cap A$$

how can we simplify this?

Several of the following set identities are similar to those in standard mathematics

This is incomplete and a draft, additional information is to be added

Discrete Mathematics/Sieve of Eratosthenes

The Sieve of Eratosthenes is a method for find prime numbers that is attributed to the ancient Greek mathematician Eratosthenes. The idea is to begin by listing all the natural numbers bigger than 2.

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24\ldots$$

and beginning with 2 we go to the first number that as not been crossed off and cross every multiple of that number that is later on in the list.

So in the case of 2, no numbers have been crossed so we start by removing every second number after 2. Our list would then look like

$$1, 2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, 21, \cancel{22}, 23, \cancel{24}\ldots$$

And we keep applying our rule. Here our next number not crossed out will be 3, we cross out every third number after 3. That will be 6, 9, 12,… and our list the becomes

$$1, 2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}\ldots$$

And so on. At the end only the prime numbers will be left.

In this case we have already found all of the primes less than 25. This is because composite numbers must always have a prime factor less than their square root. If this were not the case for some integer n we could write $n = p_1 \times p_2 \times \cdots \times p_k$. Since we are assuming n is composite we know there are at least two prime factors $p_1$and p_2. If both of which are greater than $\sqrt{n}$, then $p_1 \times p_2 > \sqrt{n} \times \sqrt{n} = n$. This would contradict that $n = p_1 \times p_2 \times \cdots \times p_k$. So for us, since we have crossed out every number with a factor smaller than 5 we have crossed out every composite number less than $5^2 = 25$.

Discrete Mathematics

Discrete mathematics is the study of mathematical structures that are fundamentally discrete rather than continuous.

Contents

- Introduction

Introductory discrete mathematics

- Set theory
- Functions and relations
- Number theory
- Logic
- Enumeration
- Graph theory
- Recursion

Upper-level discrete mathematics

Upper-level set theory

- Axiomatic set theory
- Zermelo-Frankel Axioms
- Toposes

Upper-level number theory

- Number representations
- Modular arithmetic
- Polynomials
- Finite fields
- Arithmetic Functions
- Analytic Number Theory

Upper-level logic

- Godel's incompleteness theorem
- Second order logic

Abstract algebra

Abstract algebraic systems

- Groups
- Lattice theory
- Matroids
- Boolean algebra
- Category theory

Algebra over other number systems

- Hypercomplex numbers
- Rings, fields and modules

Others

- Combinatory logic
- Languages and grammars

Automata

- Finite state automata
- Pushdown automata
- Turing machines
- Cellular automata

Further problems

- Selected problems

Unordered pages

- Axiom of choice
- Naive set theory
- Sieve of Eratosthenes

Article Sources and Contributors

Discrete Mathematics/Introduction *Source*: http://en.wikibooks.org/w/index.php?oldid=1920245 *Contributors*: Adrignola, Alsocal, Dysprosia, Jguk, The enemies of god, 11 anonymous edits

Discrete Mathematics/Set theory *Source*: http://en.wikibooks.org/w/index.php?oldid=2282673 *Contributors*: Adrignola, Arthurvogel, B9 hummingbird hovering, CloudNine, Cybermaster, Dysprosia, Fishpi, FlyingPenguins, Grendelkhan, Gruntmaster6000, Jguk, Jonathan48, MarkHudson, Matthew Low, Matthewglenadams, Nigeltn35, Panic2k4, Paul, Pribis, Pzone, Sakiv classic, Shamilj, Sigma 7, Skimpysking, Spal, The enemies of god, 132 anonymous edits

Discrete Mathematics/Set theory/Page 2 *Source*: http://en.wikibooks.org/w/index.php?oldid=2266446 *Contributors*: Adrignola, Nigeltn35, QuiteUnusual, 2 anonymous edits

Discrete Mathematics/Functions and relations *Source*: http://en.wikibooks.org/w/index.php?oldid=2282241 *Contributors*: Adrignola, AndersJansson, Avanderbergh, Avicennasis, BCW, Calberty, Cybermaster, Dysprosia, Greenbreen, Grendelkhan, JenVan, Jguk, Jomegat, Leonidas, Panic2k4, Patrick, Peter.shank, QuiteUnusual, Recent Runes, Satya Mounika, Soeb, Theresa knott, Webaware, 99 anonymous edits

Discrete Mathematics/Number theory *Source*: http://en.wikibooks.org/w/index.php?oldid=2303162 *Contributors*: Adrignola, Avicennasis, Bob A, Carandol, Cyp, Doctormatt, DragOnasdf, Dysprosia, Grendelkhan, Hagindaz, Imran, Jguk, Jleedev, Jomegat, Jonathan48, Kernigh, Konne88, Matt Deckard, Michael McGovern, MichaelPMcGovern, MikeBorkowski, Mkn, Norman Weiner, Recent Runes, SamE, Xiaodai, Évariste, 76 anonymous edits

Discrete Mathematics/Graph theory *Source*: http://en.wikibooks.org/w/index.php?oldid=2228680 *Contributors*: Adrignola, DavidCary, Dysprosia, Fermatprime, Iamunknown, Jguk, Jomegat, Kuldeep, Laleena, MikeBorkowski, Ransomw, Rich Farmbrough, SpaceMoose, Tannersf, Valentine.w, 32 anonymous edits

Discrete Mathematics/Recursion *Source*: http://en.wikibooks.org/w/index.php?oldid=2293354 *Contributors*: Adrignola, Avicennasis, Dysprosia, Eka.a.kurniawan, Jguk, QuiteUnusual, Xania, 25 anonymous edits

Discrete Mathematics/Axiomatic set theory *Source*: http://en.wikibooks.org/w/index.php?oldid=1578485 *Contributors*: Adrignola, Jguk, Siroxo, Whiteknight, 3 anonymous edits

Discrete Mathematics/Zermelo-Frankel Axioms *Source*: http://en.wikibooks.org/w/index.php?oldid=1578529 *Contributors*: Adrignola, Shahab

Discrete Mathematics/Number representations *Source*: http://en.wikibooks.org/w/index.php?oldid=2065177 *Contributors*: Adrignola, Avicennasis, Bob A, Dysprosia, Jguk, Xiaodai, 5 anonymous edits

Discrete Mathematics/Modular arithmetic *Source*: http://en.wikibooks.org/w/index.php?oldid=2103703 *Contributors*: Adrignola, Alsocal, Avicennasis, Carandol, Cyp, Dysprosia, Grendelkhan, Imran, Jguk, John254, Poolisfun, QuiteUnusual, Van der Hoorn, 42 anonymous edits

Discrete Mathematics/Polynomials *Source*: http://en.wikibooks.org/w/index.php?oldid=2254110 *Contributors*: Adrignola, Avicennasis, Carandol, Cyp, Derbeth, Dysprosia, Jguk, Recent Runes, Shahab, Thebhgg, 14 anonymous edits

Discrete Mathematics/Finite fields *Source*: http://en.wikibooks.org/w/index.php?oldid=2065173 *Contributors*: Adrignola, Avicennasis, Carandol, Dysprosia, Jguk, Jpkotta, Thenub314, 10 anonymous edits

Discrete Mathematics/Arithmetic Functions *Source*: http://en.wikibooks.org/w/index.php?oldid=1578483 *Contributors*: Adrignola, Alsocal, Jguk, 3 anonymous edits

Discrete Mathematics/Analytic Number Theory *Source*: http://en.wikibooks.org/w/index.php?oldid=2065172 *Contributors*: Adrignola, Avicennasis, Doctormatt, Jguk, The enemies of god, 13 anonymous edits

Abstract Algebra/Group Theory *Source*: http://en.wikibooks.org/w/index.php?oldid=2305110 *Contributors*: Adakkak, Adrignola, Amani, Aronbeekman, Arydye001, Ashsong, Barsamin, ComplexZeta, Dan Gardner, Dan Polansky, Davy Cielen, Drufino, Dysprosia, Elroch, Espen180, F1sdz, Fishpi, Fokion, Functor Salad, Grendelkhan, Hagindaz, Huopa, Imran, Inkling, Isomorphic, Jguk, Jmurray1022, Jomegat, Lockey, Matthewmayer, MikeBorkowski, Mjeff, Mkn, Panic2k4, Patrick, Pkazazes, Pm5, Porton, QuiteUnusual, Rcamp004, Robert Horning, Roby1984, Shahab, Sigma 7, The Scarlet Letter, Thebhgg, Thenub314, Whiteknight, Zylorian, 150 anonymous edits

Abstract Algebra/Lattice theory *Source*: http://en.wikibooks.org/w/index.php?oldid=2305100 *Contributors*: Alsocal, Jguk, Panic2k4, Sigma 7, Thenub314, 4 anonymous edits

Abstract Algebra/Matroids *Source*: http://en.wikibooks.org/w/index.php?oldid=1599000 *Contributors*: Jguk, Sigma 7, Thenub314, 4 anonymous edits

Abstract Algebra/Category theory *Source*: http://en.wikibooks.org/w/index.php?oldid=1793299 *Contributors*: Adrignola, Dysprosia, Elroch, Hoogli, J Bytheway, Jguk, Ndave, Sigma 7, Thenub314, 8 anonymous edits

Abstract Algebra/Hypercomplex numbers *Source*: http://en.wikibooks.org/w/index.php?oldid=2280946 *Contributors*: Emperorbma, Jguk, Thenub314, 4 anonymous edits

Abstract Algebra/Rings *Source*: http://en.wikibooks.org/w/index.php?oldid=2305090 *Contributors*: Avicennasis, Badanedwa, Barnaby dawson, Dysprosia, Hyad, Jguk, Ndriscoll, Panic2k4, Sigma 7, The Scarlet Letter, Thenub314, 25 anonymous edits

Discrete Mathematics/Combinatory logic *Source*: http://en.wikibooks.org/w/index.php?oldid=1578486 *Contributors*: Adrignola, Jguk, 2 anonymous edits

Discrete Mathematics/Finite state automata *Source*: http://en.wikibooks.org/w/index.php?oldid=1578489 *Contributors*: Adrignola, Etothex, Jguk, 2 anonymous edits

Discrete Mathematics/Selected problems *Source*: http://en.wikibooks.org/w/index.php?oldid=1578524 *Contributors*: Adrignola, Alsocal, Dysprosia, Jguk, 5 anonymous edits

Discrete Mathematics/Axiom of choice *Source*: http://en.wikibooks.org/w/index.php?oldid=1578484 *Contributors*: Adrignola, Jguk, 1 anonymous edits

Discrete Mathematics/Naive set theory *Source*: http://en.wikibooks.org/w/index.php?oldid=2065176 *Contributors*: Adrignola, Avicennasis, Jguk, 3 anonymous edits

Discrete Mathematics/Sieve of Eratosthenes *Source*: http://en.wikibooks.org/w/index.php?oldid=2065182 *Contributors*: Adrignola, Avicennasis, Az1568, Hagindaz, Jguk, Robert Horning, TheDaveRoss, Thenub314, 2 anonymous edits

Discrete Mathematics *Source*: http://en.wikibooks.org/w/index.php?oldid=1915382 *Contributors*: Adrignola, Dallas1278, Dysprosia, Emperorbma, Hagindaz, Icewedge, Jguk, Mike.lifeguard, Mkn, Mmmooonnnsssttteeerrr, Mrwojo, Robert Horning, Thenub314, Whiteknight, Xiaodai, 14 anonymous edits

Image Sources, Licenses and Contributors

License